CS1800 Situation Analysis

Attached is the **Huawei** Situation Analysis for CS1800. The date you are making the recommendation is March 28, 2019. Please do not consider any information released after that date.

Some things to remember:

- **Think multidimensionally**: Cyber policy impacts many different issues, and it is important to identify potential risks and opportunities in your analysis. Consider the strengths and weaknesses of several possible responses and select the optimal response.
- **Engage the scenario**: Assume that the situation which we have provided you is plausible. At the same time, think critically about the information that you have been provided and its origins.
- **Consider interests:** Organizations have a broad and diverse set of interests. How might your decision impact other interests which your organization would like to secure? If you choose one course of action, would a different office at your organization reject your approach? Be sure to be able to justify your response as strongly as possible.
- **Think holistically:** It is important to also consider not just your interests, but *all* parties' interests, including states and non-state actors.
- **Take a clear stance:** These situations are intentionally divisive, even amongst cybersecurity and policy experts. Your task is to recommend a decision, not describe the situation, so taking a strong stance and defending it is encouraged.

What you are responsible for:

1. A brief, informal oral presentation by your group in section. There are no requirements for using visual materials, nor are there requirements for how many members of your group must speak. Expect to outline your course of action for roughly five, but no more than ten, minutes.

2. Engaging in a brief Q&A from your classmates and your TAs afterwards. We will be assessing the degree to which you have prepared justifications for your course of action.

3. A brief, informal one-page summary of your proposed plan of action to be emailed to your TAs before your presentation. Formatting is not especially important – we just want a record of your approach for evaluation purposes. Bullet points are acceptable in this assignment. No bibliography is required.

4. Filling out a peer evaluation after your presentation, during which you will have the opportunity to inform the HTAs about whether all members of your group contributed fairly to your group assignment.

Included in this brief:

1. A letter from the Chancellor's office asking for your recommendation.

2. An article published by the New York Times outlining the 5G security debate.

3. The U.K.'s Huawei Cyber Security Evaluation Center (HCSEC) annual report on Huawei, edited to only include the summary and conclusions. The full report is available here.

March 28, 2019

Chancellor Merkel is considering whether to allow Huawei to be involved in Germany's 5G networks. Germany is facing pressures from both the United States and China in its decision making, and we have delayed our decision significantly more than other countries. Prolonging this period of uncertainty risks leaving Germany ill-equipped to develop 5G infrastructure, negatively impacting our economic competitiveness in the future. Thus, the Chancellor asks for your independent advice on which path to take.

Huawei has been the subject of allegations, primarily by the United States government, regarding its subservience to the Chinese government. While allegations of past or current spying are limited, there is widespread concern that China's legal system could force Huawei to utilize its position for intelligence purposes. Our own intelligence agencies concur with the assessment made by the United States that the use of Huawei in 5G networks could create national security issues in the future.

We are facing significant diplomatic pressure from both the United States and China, made more difficult by a high economic reliance on both nations. As a major export economy, we rely on both countries as markets for our motor vehicles, pharmaceuticals, advanced machinery, and other products. The continuing trade war between the U.S. and China has already damaged our economy, and the Chancellor is hesitant to take actions that will antagonize either country. The U.S. has brought into question the credibility and trustworthiness of nations which use Huawei as a security partner, which Germany is particularly sensitive to given the importance of the U.S. as a strategic partner. Chinese officials and state media, meanwhile, have promised that China will "not sit idle" if Germany blocks Huawei from its networks, promising punitive measures.

The advantage of our delay is the ability to analyze the approaches taken by other nations. Australia, for example, has banned Huawei from its networks outright, despite a high economic reliance and the presence of existing tensions with China. The United Kingdom, on the other hand, is allowing Huawei to build the "periphery" of its network, while setting up a body (the Huawei Cyber Security Evaluation Centre, or HCSEC) designed to report on and mitigate risks to national security posed by Huawei. HCSEC is yet to find any evidence of malpractice on the part of Huawei, although it has found "several hundred" serious cybersecurity vulnerabilities in Huawei products, many of which the company has not fixed.

Given the complexity of the issue, we ask that you provide us with a recommended course of action and an accompanying analysis of the risks.

The New York Times | https://nyti.ms/2S6LObM

In 5G Race With China, U.S. Pushes Allies to Fight Huawei

By David E. Sanger, Julian E. Barnes, Raymond Zhong and Marc Santora

Jan. 26, 2019

Jeremy Hunt, the British foreign minister, arrived in Washington last week for a whirlwind of meetings facing a critical question: Should Britain risk its relationship with Beijing and agree to the Trump administration's request to ban Huawei, China's leading telecommunications producer, from building its next-generation computer and phone networks?

Britain is not the only American ally feeling the heat. In Poland, officials are also under pressure from the United States to bar Huawei from building its fifth generation, or 5G, network. Trump officials suggested that future deployments of American troops — including the prospect of a permanent base labeled "Fort Trump" — could hinge on Poland's decision.

And a delegation of American officials showed up last spring in Germany, where most of Europe's giant fiber-optic lines connect and Huawei wants to build the switches that make the system hum. Their message: Any economic benefit of using cheaper Chinese telecom equipment is outweighed by the security threat to the NATO alliance.

Over the past year, the United States has embarked on a stealthy, occasionally threatening, global campaign to prevent Huawei and other Chinese firms from participating in the most dramatic remaking of the plumbing that controls the internet since it sputtered into being, in pieces, 35 years ago.

The administration contends that the world is engaged in a new arms race — one that involves technology, rather than conventional weaponry, but poses just as much danger to America's national security. In an age when the most powerful weapons, short of nuclear arms, are cyber-controlled, whichever country dominates 5G will gain an economic, intelligence and military edge for much of this century.

The transition to 5G — already beginning in prototype systems in cities from Dallas to Atlanta — is likely to be more revolutionary than evolutionary. What consumers will notice first is that the network is faster — data should download almost instantly, even over cellphone networks.

It is the first network built to serve the sensors, robots, autonomous vehicles and other devices that will continuously feed each other vast amounts of data, allowing factories, construction sites and even whole cities to be run with less moment-to-moment human intervention. It will also enable greater use of virtual reality and artificial intelligence tools.

But what is good for consumers is also good for intelligence services and cyberattackers. The 5G system is a physical network of switches and routers. But it is more reliant on layers of complex software that are far more adaptable, and constantly updating, in ways invisible to users — much as an iPhone automatically updates while charging overnight. That means whoever controls the networks controls the information flow — and may be able to change, reroute or copy data without users' knowledge.

In interviews with current and former senior American government officials, intelligence officers and top telecommunications executives, it is clear that the potential of 5G has created a zero-sum calculus in the Trump White House — a conviction that there must be a single winner in this arms race, and the loser must be banished. For months, the White House has been drafting an executive order, expected in the coming weeks, that would effectively ban United States companies from using Chinese-origin equipment in critical telecommunications networks. That goes far beyond the existing rules, which ban such equipment only from government networks.

Nervousness about Chinese technology has long existed in the United States, fueled by the fear that the Chinese could insert a "back door" into telecom and computing networks that would allow Chinese security services to intercept military, government and corporate communications. And Chinese cyberintrusions of American companies and government entities have occurred repeatedly, including by hackers suspected of working on behalf of China's Ministry of State Security.

But the concern has taken on more urgency as countries around the world begin deciding which equipment providers will build their 5G networks.

American officials say the old process of looking for "back doors" in equipment and software made by Chinese companies is the wrong approach, as is searching for ties between specific executives and the Chinese government. The bigger issue, they argue, is the increasingly authoritarian nature of the Chinese government, the fading line between independent business and the state and new laws that will give Beijing the power to look into, or maybe even take over, networks that companies like Huawei have helped build and maintain.

"It's important to remember that Chinese company relationships with the Chinese government aren't like private sector company relationships with governments in the West," said William R. Evanina, the director of America's National Counterintelligence and Security Center. "China's 2017 National Intelligence Law requires Chinese companies to support, provide assistance and cooperate in China's national intelligence work, wherever they operate."

The White House's focus on Huawei coincides with the Trump administration's broader crackdown on China, which has involved sweeping tariffs on Chinese goods, investment restrictions and the indictments of several Chinese nationals accused of hacking and cyberespionage. President Trump has accused China of "ripping off our country" and plotting to grow stronger at America's expense.

Mr. Trump's views, combined with a lack of hard evidence implicating Huawei in any espionage, have prompted some countries to question whether America's campaign is really about national security or if it is aimed at preventing China from gaining a competitive edge.

Administration officials see little distinction in those goals.

"President Trump has identified overcoming this economic problem as critical, not simply to right the balance economically, to make China play by the rules everybody else plays by, but to prevent an imbalance in political/military power in the future as well," John R. Bolton, Mr. Trump's national security adviser, told The Washington Times on Friday. "The two aspects are very closely tied together in his mind."

The administration is warning allies that the next six months are critical. Countries are beginning to auction off radio spectrum for new, 5G cellphone networks and decide on multibillion-dollar contracts to build the underlying switching systems. This past week, the Federal Communications Commission announced that it had concluded its first high-band 5G spectrum auction.

The Chinese government sees this moment as its chance to wire the world — especially European, Asian and African nations that find themselves increasingly beholden to Chinese economic power.

"This will be almost more important than electricity," said Chris Lane, a telecom analyst in Hong Kong for Sanford C. Bernstein. "Everything will be connected, and the central nervous system of these smart cities will be your 5G network."

Both the United States and China believe that whichever country dominates 5G will gain an economic, intelligence and military edge for much of this century. Fred Dufour/Agence France-Presse — Getty Images

A New Red Scare?

So far, the fear swirling around Huawei is almost entirely theoretical. Current and former American officials whisper that classified reports implicate the company in possible Chinese espionage but have produced none publicly. Others familiar with the secret case against the company say there is no smoking gun — just a heightened concern about the firm's rising technological dominance and the new Chinese laws that require Huawei to submit to requests from Beijing.

Ren Zhengfei, Huawei's founder, has denied that his company spied for China. "I still love my country. I support the Communist Party of China. But I will never do anything to harm any other nation," he said earlier this month.

Australia last year banned Huawei and another Chinese manufacturer, ZTE, from supplying 5G equipment. Other nations are wrestling with whether to follow suit and risk inflaming China, which could hamper their access to the growing Chinese market and deprive them of cheaper Huawei products.

Government officials in places like Britain note that Huawei has already invested heavily in older-style networks — and has employed Britons to build and run them. And they argue that Huawei isn't going away — it will run the networks of half the world, or more, and will have to be connected, in some way, to the networks of the United States and its allies.

Yet BT Group, the British telecom giant, has plans to rip out part of Huawei's existing network. The company says that was part of its plans after acquiring a firm that used existing Huawei equipment; American officials say it came after Britain's intelligence services warned of growing risks. And Vodafone Group, which is based in London, said on Friday that it would temporarily stop buying Huawei equipment for parts of its 5G network.

Nations have watched warily as China has retaliated against countries that cross it. In December, Canada arrested a top Huawei executive, Meng Wanzhou, at the request of the United States. Ms. Meng, who is Mr. Ren's daughter, has been accused of defrauding banks to help Huawei's business evade sanctions against Iran. Since her arrest, China has detained two Canadian citizens and sentenced to death a third Canadian, who had previously been given 15 years in prison for drug smuggling.

"Europe is fascinating because they have to take sides," said Philippe Le Corre, nonresident senior fellow at the Carnegie Endowment for International Peace. "They are in the middle. All these governments, they need to make decisions. Huawei is everywhere."

A Huawei store in Warsaw. This month, the Polish government made two high-profile espionage arrests, including an employee of Huawei. Maciek Nabrdalik for The New York Times

Growing Suspicions

This month, the Polish government made two high-profile espionage arrests: a former intelligence official, Piotr Durbajlo, and Wang Weijing, an employee of Huawei. The arrests are the strongest evidence so far that links Huawei with spying activities.

Mr. Wang, who was quickly fired by Huawei, has been accused of working for Chinese intelligence agencies, said a top former Polish intelligence official. Mr. Wang, according to American diplomats, was the handler of Mr. Durbajlo, who appears to have helped the Chinese penetrate the Polish government's most secure communications network.

A senior American official said the case was a prime example of how the Chinese government plants intelligence operatives inside Huawei's vast global network. Those operatives potentially have access to overseas communications networks and can conduct espionage that the affected companies are not aware of, the official said.

Huawei said Mr. Wang had brought "disrepute" on the company and his actions had nothing to do with its operations.

Mr. Wang's lawyer, Bartlomiej Jankowski, says his client has been caught up in a geopolitical tug of war between the United States and China.

American and British officials had already grown concerned about Huawei's abilities after cybersecurity experts, combing through the company's source code to look for back doors, determined that Huawei could remotely access and control some networks from the company's Shenzhen headquarters.

On careful examination, the code that Huawei had installed in its network-control software did not appear to be malicious. Nor was it hidden. It appeared to be part of a system to update remote networks and diagnose trouble. But in some circumstances, it could also route traffic around corporate data centers — where firms monitor and control their networks — and its mere existence is now cited as evidence that hackers or Chinese intelligence could use Huawei equipment to penetrate millions of networks.

American officials and academics say Chinese telecommunications companies have also temporarily hijacked parts of the internet, rerouting basic traffic from the United States and Canada to China.

One academic paper, co-written by Chris C. Demchak, a Naval War College professor, outlined how traffic from Canada meant for South Korea was redirected to China for six months. That 2016 attack has been repeated, according to American officials, and provides opportunity for espionage.

Last year, AT&T and Verizon stopped selling Huawei phones in their stores after Huawei begin equipping the devices with its own sets of computer chips — rather than relying on American or European manufacturers. The National Security Agency quietly raised alarms that with Huawei supplying its own parts, the Chinese company would control every major element of its networks. The N.S.A. feared it would no longer be able to rely on American and European providers to warn of any evidence of malware, spying or other covert action.

An assembly line at Huawei's cellphone plant in Dongguan, China. The company has already surpassed Apple as the world's second biggest cellphone provider. Qilai Shen/Bloomberg

The Rise of Huawei

In three decades, Huawei has transformed itself from a small reseller of low-end phone equipment into a global giant with a dominant position in one of the crucial technologies of the new century.

Last year, Huawei edged out Apple as the second-biggest provider of cellphones around the world. Richard Yu, who heads the company's consumer business, said in Beijing several days ago that "even without the U.S. market we will be No. 1 in the world," by the end of this year or sometime in 2020.

The company was founded in 1987 by Mr. Ren, a former People's Liberation Army engineer who has become one of China's most successful entrepreneurs.

American officials say the company started through imitation, and even theft, of American technology. Cisco Systems sued Huawei in 2003, saying it had illegally copied the American company's source code. The two companies settled out of court.

But Huawei did not just imitate. It opened research centers (including one in California) and built alliances with leading universities around the world. Last year, it generated $100 billion in revenue, twice as much as Cisco and significantly more than IBM. Its ability to deliver well-made equipment at a lower cost than Western firms drove once-dominant players like Motorola and Lucent out of the telecom-equipment industry.

While American officials refuse to discuss it, the government snooping was a two-way street. As early as 2010, the N.S.A. secretly broke into Huawei's headquarters, in an operation, code-named "Shotgiant," a discovery revealed by Edward J. Snowden, the former N.S.A. contractor now living in exile in Moscow.

Documents show that the N.S.A. was looking to prove suspicions that Huawei was secretly controlled by the People's Liberation Army — and that Mr. Ren never really left the powerful army unit. It never found the evidence, according to former officials. But the Snowden documents also show that the N.S.A. had another goal: to better understand Huawei's technology and look for potential back doors. This way, when the company sold equipment to American adversaries, the N.S.A. would be able to target those nations' computer and telephone networks to conduct surveillance and, if necessary, offensive cyberoperations.

In other words, the Americans were trying to do to Huawei the exact thing they are now worried Huawei will do to the United States.

President Trump met with Andrzej Duda, his Polish counterpart, last year. Mr. Duda has suggested that the United States build a $2 billion base and training area, which Mr. Duda only half-jokingly called "Fort Trump." Doug Mills/The New York Times

A Global Campaign

After an uproar in 2013 about Huawei's growing dominance in Britain, the country's powerful Intelligence and Security Committee, a parliamentary body, argued for banning Huawei, partly because of Chinese cyberattacks aimed at the British government. It was overruled, but Britain created a system to require that Huawei make its hardware and source code available to GCHQ, the country's famous code-breaking agency.

In July, Britain's National Cyber Security Center for the first time said publicly that questions about Huawei's current practices and the complexity and dynamism of the new 5G networks meant it would be difficult to find vulnerabilities.

At roughly the same time, the N.S.A., at a series of classified meetings with telecommunications executives, had to decide whether to let Huawei bid for parts of the American 5G networks. AT&T and Verizon argued there was value in letting Huawei set up a "test bed" in the United States since it would have to reveal the source code for its networking software. Allowing Huawei to bid would also drive the price of building the networks down, they argued.

The director of the N.S.A. at the time, Adm. Michael S. Rogers, never approved the move and Huawei was blocked.

In July 2018, with these decisions swirling, Britain, the United States and other members of the "Five Eyes" intelligence-sharing alliance met for their annual meeting in Halifax, Nova Scotia, where Chinese telecommunications companies, Huawei and 5G networks were at the top of the agenda. They decided on joint action to try to block the company from building new networks in the West.

American officials are trying to make clear with allies around the world that the war with China is not just about trade but a battle to protect the national security of the world's leading democracies and key NATO members.

On Tuesday, the heads of American intelligence agencies will appear before the Senate to deliver their annual threat assessment, and they are expected to cite 5G investments by Chinese telecom companies, including Huawei, as a threat.

In Poland, the message has quietly been delivered that countries that use Chinese telecommunications networks would be unsafe for American troops, according to people familiar with the internal discussions.

That has gotten Poland's attention, given that its president, Andrzej Duda, visited the White House in September and presented a plan to build a $2 billion base and training area, which Mr. Duda only half-jokingly called "Fort Trump."

Col. Grzegorz Malecki, now retired, who was the head of the Foreign Intelligence Agency in Poland, said it was understandable that the United States would want to avoid potentially compromising its troops.

"And control over the 5G network is such a potentially dangerous tool," said Mr. Malecki, now board president of the Institute of Security and Strategy. "From Poland's perspective, securing this troop presence outweighs all other concerns."

Adam Satariano, Joanna Berendt and Katie Benner contributed reporting.

A version of this article appears in print on Jan. 27, 2019, Section A, Page 1 of the New York edition with the headline: U.S. Scrambles to Outrun China in New Arms Race

HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2019

A report to the National Security Adviser of the United Kingdom

March 2019

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

1. This is the fifth annual report from the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei Technologies (UK) Co Ltd (Huawei UK), whose parent company, Huawei Technologies Co Ltd, is a Chinese headquartered company which is now one of the world's largest telecommunications providers.

2. HCSEC has been running for eight years. It opened in November 2010 under a set of arrangements between Huawei and Her Majesty's Government (HMG) to mitigate any perceived risks arising from the involvement of Huawei in parts of the United Kingdom's (UK) critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK telecommunications market. Through HCSEC, the UK Government is provided with insight into Huawei's UK strategies and product ranges. The UK's National Cyber Security Centre (NCSC, and previously Government Communications Headquarters (GCHQ)), as the national technical authority for information assurance and the lead Government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters.

3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure of the Oversight Board has not changed significantly, but membership has changed in 2018. Mainly, this is due to staff rotations in both HMG and Huawei positions.

4. The Oversight Board has now completed its fifth full year of work. In doing so it has covered several areas of HCSEC's work over the course of the year. The full details of this work are set out in Part II of this report. In this summary, the main highlights are:

    i. **New secure premises for HCSEC completed** - the previously reported acquisition of new premises for HCSEC had experienced some commercial delays, but has now completed successfully and the new facilities are fully operational;

    ii. **The NCSC Technical Competence Review found that the capability of HCSEC has improved in 2018**, and the quality of staff has not diminished, meaning that technical work relevant to the overall mitigation strategy can be performed at scale and with high quality;

    iii. **The fifth independent audit of HCSEC's ability to operate independently of Huawei HQ has been completed**, with – again – no high or medium priority findings. The audit report identified one low-rated finding, relating to delivery of information and equipment within agreed Service Level Agreements. Ernst & Young concluded that there were no major concerns and the Oversight Board is satisfied that HCSEC is operating in line with the 2010 arrangements between HMG and the company;

    iv. **Further significant technical issues have been identified in Huawei's engineering processes,** leading to new risks in the UK telecommunications networks;

    v. **No material progress has been made by Huawei in the remediation of the issues reported last year,** making it inappropriate to change the level of assurance from last year or to make any comment on potential future levels of assurance.

5. The key conclusions from the Oversight Board's fifth year of work are:

i. In 2018, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks;

ii. However, as reported in 2018, **HCSEC's work has continued to identify concerning issues in Huawei's approach to software development** bringing significantly increased risk to UK operators, which requires ongoing management and mitigation;

iii. **No material progress** has been made on the issues raised in the previous 2018 report;

iv. The Oversight Board continues to be able to provide **only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK;

v. The Oversight Board advises that **it will be difficult to appropriately risk-manage future products** in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated;

vi. At present, the Oversight Board has **not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation programme** that it has proposed as a means of addressing these underlying defects. The Board will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC;

vii. Overall, the Oversight Board can **only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term.**

SECTION V: Conclusions

5.1 The Oversight Board has now completed its work during this period. Its five meetings and its work out of Committee have provided a useful enhancement of the governance arrangements for HCSEC.

5.2 The Oversight Board has concluded that in the year 2018, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks.

5.3 However, as reported in 2018, HCSEC's work continues to identify **significant, concerning issues** in Huawei's approach to software development bringing significantly increased risk to UK operators, which requires ongoing management and mitigation. Operators will need to take into account the mitigations required as a result of the extensive vulnerability and software engineering and cyber security quality information provided by the work of HCSEC.

5.4 No material progress has been made on the issues raised in the 2018 report and further issues have come to light in this year's report. **The Oversight Board continues to be able to provide only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK. The Oversight Board notes in particular the following advice from NCSC:

i. That there remains no end-to-end integrity of the products as delivered by Huawei and limited confidence on Huawei's ability to understand the content of any given build and its ability to perform true root cause analysis of identified issues. This raises significant concerns about vulnerability management in the long-term;

ii. That Huawei's software component management is defective, leading to higher vulnerability rates and significant risk of unsupportable software;

iii. That although the review of subsequent major versions of the eNodeB showed improvements in code duplication and a significant reduction in the number of copies of the OpenSSL component, the general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects.

5.5 The Oversight Board advises that it will be difficult to appropriately risk manage future products in the context of UK deployments, until Huawei's software engineering and cyber security processes are remediated. **The Oversight Board currently has not seen anything to give it confidence in Huawei's ability to bring about change via its transformation programme** and will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC.

5.6 Huawei's transformation plan could in principle be successful, bringing Huawei's software engineering and cyber security processes up to current industry good practice. Huawei's own public estimates are that this transformation will take three to five years. The Oversight Board would require NCSC assessment of evidence of sustained change across multiple versions of multiple products in order to have confidence in success – a single version of a single product with better objective engineering quality and security does not guarantee a successful and sustainable change across the company, or even in that individual product group.

5.7 The evidence of sustained change is especially important as similar strongly worded commitments from Huawei in the past have not brought about any discernible improvements. The Oversight Board note in particular the commitments first made in Huawei's 2012 cyber security whitepaper (accessible at https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/cyber-security-white-paper-2012-en.pdf) and repeated subsequently. Therefore, significant and sustained evidence will be required to give the Oversight Board any confidence that Huawei's transformation programme will bring about the required change.

5.8 It should be made clear that the Oversight Board's statement of limited assurance is not a comment on the security of the UK's networks today, which is a matter for individual operators, Ofcom, DCMS and NCSC. It is assurance as to

whether HCSEC can continue to provide security relevant artefacts to inform UK stakeholders as part of the mitigation strategy. The oversight provided for in our mitigation strategy for Huawei's presence in the UK is arguably the toughest and most rigorous in the world. This report does not, therefore, suggest that the UK networks are more vulnerable than last year. Indeed, the significant technical insight provided by HCSEC to the UK operators allows them to plan more effective mitigations. The report from the Oversight Board states only that Huawei's development and support processes are not currently conducive to long-term security risk management and, at present, the Oversight Board has seen nothing to give confidence in Huawei's capacity to fix this.

5.9 These conclusions of the Oversight Board do not presage in any way the review of telecoms supply arrangements in the UK currently being carried out by DCMS on behalf of Government with the aim of ensuring there is an effective policy framework in place for the deployment of secure and resilient 5G and full fibre networks. DCMS has stated that the review will carefully consider the Oversight Board's findings and conclusions on technical assurance, alongside other evidence, in the development of policy. But the review will be based on a diverse set of evidence of which the Oversight Board conclusions are only a part.

5.10 Finally, it should also be noted that the Oversight Board wishes to emphasise that it has no remit to direct or influence the purchasing decisions of the UK operators. They must individually manage the risk in their own networks, with support from Ofcom, DCMS and NCSC.

5.11 The Oversight Board hopes that this report continues to add to Parliamentary – and through it, public – knowledge of the operation of the arrangements and the transparency with which they are operated.

~~~~
~~~~