INTRINSEC
Innovative by design

Cyber Threat Intelligence

China: Vulnerabilities as a strategic resource

@Intrinsec @Intrinsec Blog Website

Table of contents

Key findings

This report presents:

- The Regulations on the Management of Network Product Security Vulnerabilities (RMSV), an extension of China's 2017 Cybersecurity Law, targeting hardware/software companies as well as cybersecurity researchers.
- The RMSV prohibits the illegal collection, sale or disclosure of vulnerability information "that may endanger the security of information systems".
- The same regulation requires companies to have a system for communicating discovered vulnerabilities, with an obligation to keep logs for a period of six months.
- The RMSV imposes strict rules on the disclosure and publication of vulnerabilities, prohibiting any detailed public communication without the consent of the Ministry of Public Security during periods of major Chinese activity.
- Companies are obliged to audit, communicate to the government and correct any vulnerabilities discovered within 48 hours.
- Network product providers are encouraged to set up "Bug Bounty" type programmes to encourage the discovery and privatisation of vulnerabilities.
- China is aiming to centralise the collection of vulnerabilities, by prohibiting its researchers from taking part in conferences abroad and by developing public-private partnerships.
- The submission of vulnerabilities to the national database includes the provision of proof-of-concept, i.e. code enabling the existence of the said vulnerability to be demonstrated.
- The entity behind the national database promises rewards proportional to the quality of the information submitted.
- A statistical analysis of data relating to the vulnerabilities submitted reveals a drop in submissions to the China National Vulnerability Database (CNVD) and an obfuscation of data on the side of the China National Vulnerability Database of Information Security (CNNVD), suggesting a strategic exploitation of vulnerabilities by the Chinese government.

Introduction

Since the emergence of the ARPANET project, the world of cybersecurity has been in a constant state of evolution. Its environment - both digital and legal - is not always favourable to the most peaceful development of its ecosystem. The emergence of a more secure and transparent cyberspace is often hindered by aggressive state ideologies. Some of these ideologies - driven by a desire to gain power and economic growth - are very often openly justified by the need to improve national security. Closely interlinked with espionage and intelligence, these state intentions take the form of support for intrusion sets, as well as lawfare actions.

The Chinese Constitution of 1982 - the founding text of the People's Republic of China (PRC) - defines the Chinese regime as "*a socialist state of people's democratic dictatorship, led by the working class and based on the alliance of workers and peasants*". Its second paragraph explicitly prohibits "*any organisation or individual from attempting to undermine it*". This firm stance on preserving the regime will adopt virtually no limits.

Still in the same spirit of national security - at least in appearance - the Chinese government intends to develop the means at its disposal to control and retain control over what happens on its territory. In addition, the development of its legal arsenal with extraterritorial reach will cause some concern on the international scene.

The Chinese administrative apparatus, in particular the Cyberspace Administration of China (CAC - formerly SIIO), the Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT), will jointly be developing a wide range of restrictive legislation aimed at individuals and companies.

I. A dense and aggressive legal framework

In 1998, the "Great Firewall" appeared following the adoption of law CL97 by China's National People's Congress. As the first law tackling cyberspace, it encouraged self-censorship among legal subjects. This law requires the use of a firewall to actively filter incoming and outgoing Chinese internet traffic. It even goes as far as to detect the use of VPNs (Virtual Private Networks) and place them on IP address blocking lists. This detection mechanism then *de facto* prevents the main means for its nationals to bypass the control of the "Great Firewall". Its capacity of action - already extremely broad - will continue to grow, thanks in particular to the 2017 Intelligence Act. This firewall would thus be able to allow government bodies to carry out man-in-the-middle attacks. An interesting aspect of the 2017 law is the obligation placed on citizens and organisations to cooperate with intelligence agencies. This places all Chinese residents in a position to be the source of spying. A population at the total service of its government.

In the footsteps of this instrument, the Cybersecurity Law entered into effect in 2017. While offering new originalities in its approach to cybersecurity issues, this law will focus primarily on cross-border data transfer, as well as the storage and protection of users' personal data located in China. By imposing strict conditions around these elements, this law will act as a strong deterrent to any infringement by imposing extremely heavy penalties (imprisonment; administrative fines; withdrawal of operating rights; etc.).

For example, on 28 February 2024, a supermarket chain in the city of Nanchang saw its IT infrastructure compromised and used by an intrusion set for DDoS attacks. The supermarket chain was ordered to pay an administrative fine of 50,000 yuan (approx. €6,500), and the person directly responsible for the network 10,000 yuan (approx. €1,500). These two penalties would be based on articles 21 & 25 of the law on cybersecurity.

Article 21 states that it is necessary for all companies to apply appropriate technical measures in terms of network security in order to prevent "*interference, damage or unauthorised access*" to the infrastructure, as well as *de facto* preventing the "*leakage, theft or alteration of data*" internal to the infrastructure. Article 25 also requires each company to contact the authorities in the event of a network incident, and at the same time to apply a pre-defined emergency protocol to respond to the incident.

Such severity in the sanctions resulting from this event would be unthinkable under French and, more broadly, Western legislation - which focuses on pedagogy and prevention - except in the event of deliberate compromise of the infrastructure. The situation resulting from this law clearly demonstrates China's desire to erect an ultra-secure and controlled environment in which there is no respite for players in the digital world, and where severity is the spearhead.

But as we shall see later, this desire for a totally secure cyber ecosystem, protected from any outside interference, could in fact be hiding an entirely different desire. Behind this acceleration in securing the country's internal infrastructures, China will at the same time make progress in its objective of controlling and absorbing data, both internal and external.

In order to widen its scope of action even further, it is important to note that the 2017 Cybersecurity Law uses a range of vague and ambiguous terms in its corpus, giving it considerable latitude in the interpretation that will be made of these terms by the country's political and judicial authorities. One example is "network operators", which can be used to target all actors in the digital and technological environment.

The marker of this latitude sometimes turns into a real compliance headache for businesses. For example, on the subject of cross-border data transfer, the specification on the security of personal information - published in 2020 - offers clarification on how data should be used and stored. However, there are still substantial ambiguities. In September 2023, after a considerable amount of debate, China will propose a final set of draft regulations. At the heart of numerous debates, this draft will attempt to make the pre-existing regulations more flexible, with the aim of limiting the concerns expressed by companies operating in China due to the difficulty of achieving the objectives set by the 2017 cybersecurity law. Subjectively more flexible, this draft regulation proposes new conditions, notably concerning the self-assessment - by companies - of the sensitivity of outbound data, and the final control carried out by the Chinese authorities.

Already proposing to cover far more than its own nationals, this 2017 law will serve as a breeding ground for what will become the bugbear of companies all over the world. Our attention will now turn towards the Regulation on the Management of Network Product Security Vulnerabilities (RMSV). This 2021 text, which follows on from the 2017 cybersecurity law, enables the government to seize a strategic resource: **vulnerabilities**.

With this law, China aims to protect its infrastructures and its regime beyond its borders directly by forcing companies operating on its territory to cooperate.

II. A legislation that facilitates the massive harvesting of vulnerabilities

As a new arena for gathering intelligence, cyberspace is gradually encouraging states to acquire the specialists and technologies they need to achieve their new offensive and defensive ambitions. Some ambitions, for example, are aimed at preventing the emergence of future threats - even though international law does not recognise preventive self-defence - while others are aimed at pre-positioning critical infrastructures so as to strike at the most opportune moment.

As a true extension of the power of the State, and a leverage for the intrusion sets that they can support, the cyber weapons constituted by zero-day & one-day vulnerabilities provide an indisputable strategic advantage and almost unlimited modularity to their possessors. This is the main environment in which the RMSV operates. As stated in its **first article**, this is the latest extension to date of the Chinese Cybersecurity Law of 2017.

The **second article** of the regulation sets out the scope of application, targeting hardware and software companies operating on the territory of the People's Republic of China (PRC). Legally, it will target them generically as "network operators" or "product providers". But this second article goes even further by also targeting researchers and entities specialising in the discovery and disclosure of vulnerabilities. The entire cybersecurity sector therefore seems to be directly targeted by this regulation.

Article 4 will specify that the physical and moral persons mentioned above must not, under any circumstances, illegally collect, sell or disclose any information about a vulnerability if it has the capacity to "endanger" the security of information systems. *De facto*, this article makes illegal any collection of information considered as such by the PRC, and places in a situation of total exclusivity the official method of disclosing vulnerabilities.

As an extension of this, Article 4 prohibits any form of technical assistance or remuneration to entities exploiting vulnerabilities. Following this logic, it would be illegal for a victim to pay a ransom resulting from a compromise by ransomware following the exploitation of a vulnerability in the targeted information system. Furthermore, it would also be prohibited to buy a proof of concept (POC) of a vulnerability on one of the underground forums in order to study how it works and remedy the vulnerability more quickly.

Article 5 seems to mitigate this obvious impression of isolation. It imposes on companies to set up a system for notifying them of any information about vulnerabilities in their products discovered by an individual or a third-party company. This obligation is accompanied by a requirement to keep logs for a minimum period of six months. Under **Article 10** of the RMSV, the existence of these reporting platforms - whether created on the initiative of individuals or as a result of an obligation - must be registered with the MIIT.

Article 6 continues in this direction by strongly encouraging organisations and individuals specialising in the cybersecurity sector to inform network product providers without delay of any vulnerability discovered in any of their products.

Article 7 will also encourage network product providers to set up programmes comparable to "Bug Bounty" to reward the discovery of vulnerabilities. This process - which is widely used - makes it possible to seal off digital infrastructures as efficiently as possible by proactively searching for vulnerabilities, while reducing as much as possible the risk of this information becoming a threat if it were to be published or sold on parallel markets.

This article goes much further, however, by imposing the first specific management obligations for vulnerabilities acquired by network operators and product providers. It is these obligations that will be the focus of our attention. Finally, from these first few elements introducing the RMSV, it is already possible to detect its wide range of application, itself prey to extensive interpretation and forcibly placing its legal subjects in autarky with only one possible escape route, the China National Vulnerability Database of Information Security (CNNVD).

III. An obligation to disclose

Before continuing to present the RMSV and its management obligations, it is important to briefly present the two existing Chinese databases whose purpose is to reference the vulnerabilities reported to them, the **CNVD** and the **CNNVD**. Normally - like the National Vulnerability Database in the United States - these two databases focus on prevention through the public dissemination of information about vulnerable products. This disclosure enables exposed entities and individuals to react before any type of compromise occurs.

The **China National Vulnerability Database (CNVD)** is managed by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), a supposedly non-governmental entity. The second database, the **China National Vulnerability Database of Information Security (CNNVD)**, is administered by the China Information Technology Security Evaluation Center (CNITSEC), a government entity. CNITSEC is in fact the front office of the 13th Bureau of the Ministry of State Security (MSS), one of China's intelligence agencies.

According to the RMSV, the CNNVD is synchronised with the CNVD, suggesting that the Chinese government wishes to make the CNNVD the country's main database.

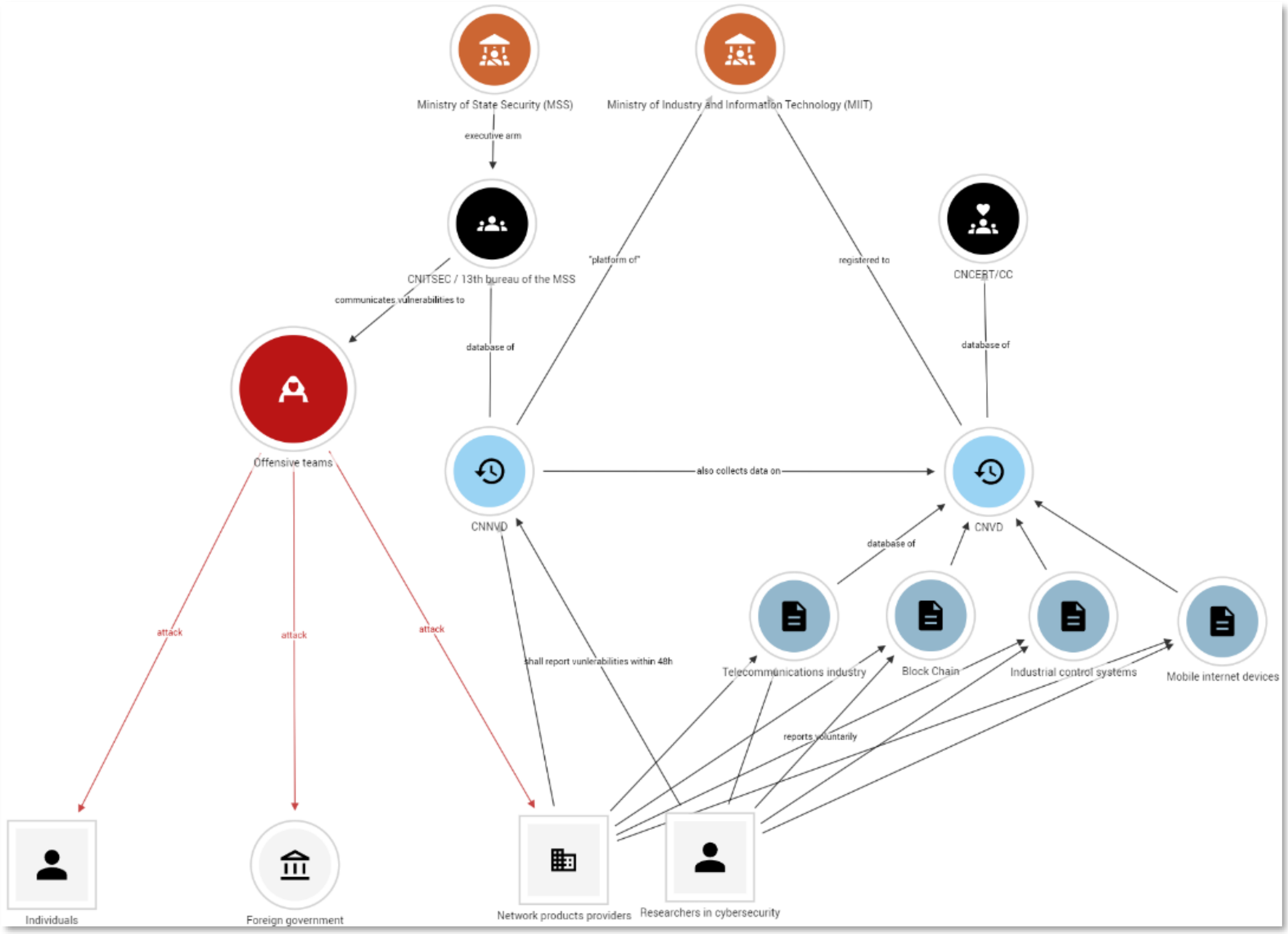

Ministry of State Security (MSS)
Ministry of Industry and Information Technology (MIIT)
executive arm
CNITSEC / 13th bureau of the MSS
"platform of"
registered to
CNCERT/CC
communicates vulnerabilities to
database of
database of
Offensive teams
CNNVD
also collects data on
CNVD
database of
attack
attack
attack
shall report vulnerabilities within 48h
Telecommunications industry
Block Chain
Industrial control systems
Mobile internet devices
reports voluntarily
Individuals
Foreign government
Network products providers
Researchers in cybersecurity

Figure 1 : Presumed organisation around the two Chinese databases (CNVD and CNNVD)

As previously mentioned, **Article 7** of the RMSV requires network operators and product providers to follow a clearly defined management protocol. This would have the dual purpose of ensuring that vulnerabilities are rapidly corrected and guiding users of affected products to apply preventive measures. Considered to be a "reasonable" protocol, it will result in a disclosure obligation being imposed on companies with infrastructures or developing their activities on Chinese territory.

- As a first action, after discovering or learning of the existence of a vulnerability, the entity concerned must carry out a security audit with the aim of testing and assessing the severity of the vulnerability. If the vulnerability involves another company - for example, through implementation in a third-party solution - the company with the vulnerable product must inform it without delay.
- Within 48 hours of its discovery, information concerning the vulnerability must be communicated to the CNNVD. The technical characteristics of the vulnerability, the threat it

represents and its impact must be included in the report. As we shall see, this list is not exhaustive, and its main purpose is not actually prevention.
- It is only once these first two phases have been completed that the company must finally proceed to correct the vulnerability and, if necessary, propose the publication of a patch. In addition, the company must also inform its users of the risks involved in using the vulnerable product, and should not hesitate to provide technical assistance to the customer if necessary.

On the question of cybersecurity experts, while ensuring that their actions are guided by "***necessity, veracity, objectivity and interest in the prevention of network security risks***", Article 9 requires them:

- Not to publish any information about any vulnerability before the company with the vulnerable product has been informed and has taken the appropriate measures to remedy the situation.
- However, if they consider that it is necessary to publish information relating to the vulnerability quickly and in advance, they must conjointly assess the vulnerability with the network product provider concerned and draw up a report addressed to the MIIT and the MPS. It is only then that the ministries mentioned above will publish the information on the CNNVD after having made their own assessment. This provision reaffirms this desire to privatise and control information.
- Any public communication concerning the detailed circumstances of the discovery and use of the vulnerability (e.g. a POC) remains prohibited.
- Finally, the use of this information for personal or collaborative purposes is formally prohibited, all the more so if it is used for "malicious" purposes (e.g. the publication of tools or procedures enabling the vulnerability to be abused; the aggravation of the vulnerability; its use to commit fraud or extortion; any "sensationalism" surrounding the vulnerability; etc.).

This article will be completed by two final prohibitions. The first concerns the communication of information relating to discovered vulnerabilities to foreign organisations or persons other than the network product provider concerned, as long as this information is not publicly disclosed on the CNNVD.

The second concerns the prohibition on the publication of details of a vulnerability without the express consent of the MPS during periods when the Chinese State is hosting major activities. The PRC is thus ensuring greater stability for its infrastructures during events such as the Olympic Games, which took place in Beijing - China - just 5 months after the regulation came into application.

Article 11 of the RMSV will require organisations specialising in the discovery of vulnerabilities to adopt internal measures designed to prevent the leakage of information, while providing a more secure working environment.

In the event of non-compliance with the RMSV's measures, **Articles 12 to 14** refer to the Cybersecurity Act 2017, specifically Articles 59; 60; 62 and 63. The latter spell out the sanctions to which the entities and individuals covered by the regulation are exposed in the event of non-compliance. They are particularly severe, and once again strengthen the grip of the regulation on researchers and companies.

Ultimately, the RMSV seems to reflect the desire of government bodies to become the central element in the harvesting of vulnerabilities. Janus-faced, in its public statements about protecting its population from the dangers of vulnerabilities, the RMSV is in fact aimed at using this sensitive information to target international society, and sometimes even its own territory.

As we have seen from the i-SOON data leak and other past events, China seems to have put in place a number of means to facilitate the harvesting of zero-day vulnerabilities. The main way is through Capture the Flag (CTF) events, which allow the government - and its branches - to harvest vulnerabilities and find new talent. The Matrix Cup - sponsored by cybersecurity company Qihoo 360 - was the latest event to take place on Chinese territory on 26 June.

By prohibiting its own cybersecurity researchers from taking part in conferences abroad, and by developing public-private partnerships, China finally seems to have legally completed its desire to privatise and capture zero-day vulnerabilities by promulgating this regulation.

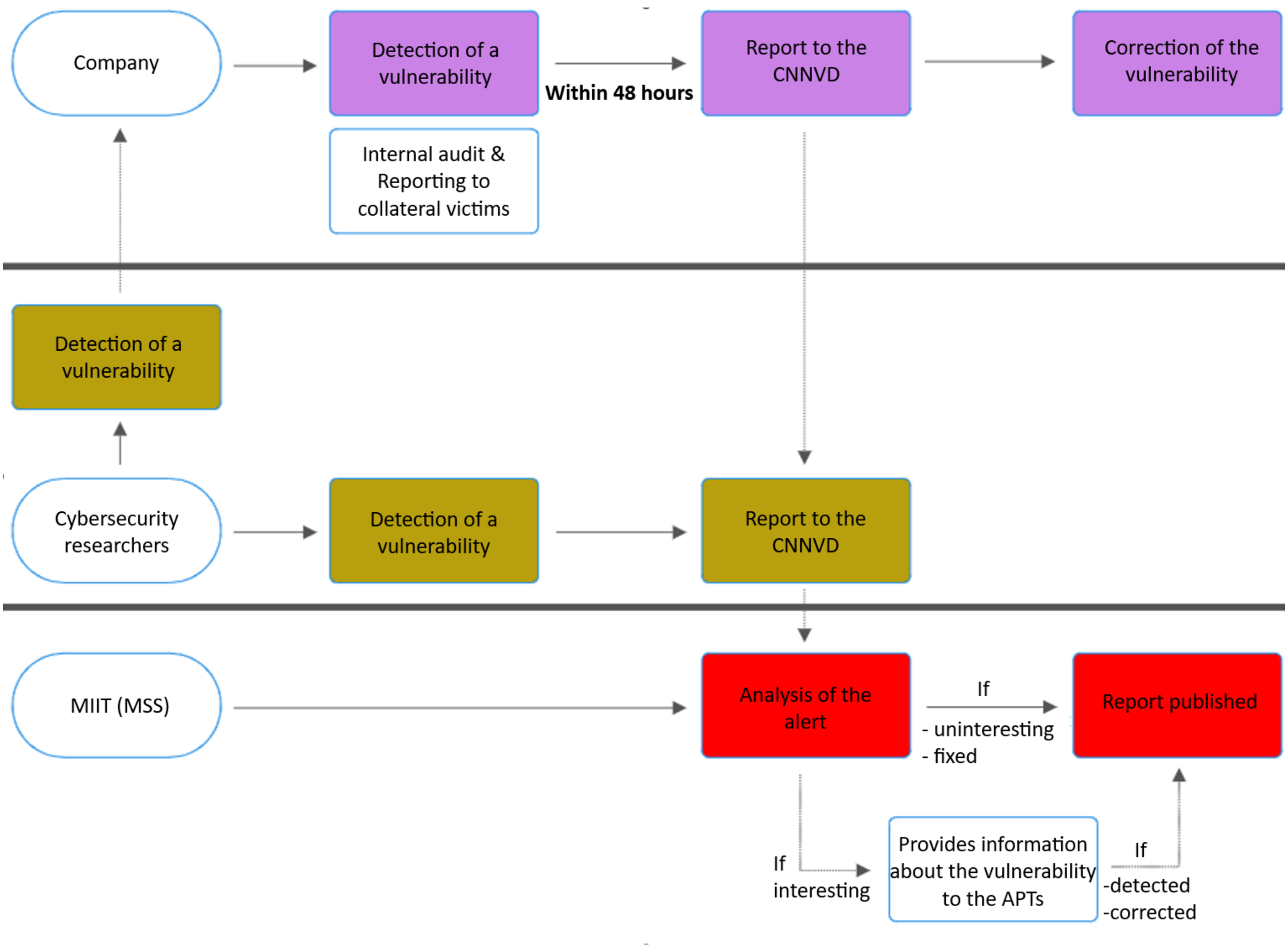

Company
Detection of a vulnerability
Within 48 hours
Report to the CNNVD
Correction of the vulnerability
Internal audit & Reporting to collateral victims
Detection of a vulnerability
Cybersecurity researchers
Detection of a vulnerability
Report to the CNNVD
MIIT (MSS)
Analysis of the alert
If
- uninteresting
- fixed
Report published
If interesting
Provides information about the vulnerability to the APTs
If
-detected
-corrected

Figure 2 : Supposed chronological diagram

IV. Voluntary collaboration or blind trust in the submission of information

As the RMSV requires all companies to communicate their own vulnerabilities, whether they have discovered them themselves or through cybersecurity researchers, its submission process to the CNNVD is intriguing on a variety of points. It reveals the real intentions behind the CNITSEC database, which the United States believes is actually hiding the MSS.

During a test involving the submission of information relating to a fictitious vulnerability, two elements not covered in the RMSV caught the attention of Intrinsec's CTI team. The CNNVD encourages the submission of a POC that could lead to an "easy reproduction" of the vulnerability. This encouragement is surprisingly accompanied by the promise of a "reward" proportional to the quality of the information submitted.

Put in the context of the existing collaboration - already highlighted in the past - between the MSS and the government-sponsored intrusion sets, it is with a medium level of confidence that we can indicate that the MSS harvests directly exploitable vulnerabilities through the CNNVD in order to pass them to the various Chinese intrusion sets.

« ***Key points to note when reporting vulnerabilities***

Please read these instructions carefully before submitting a vulnerability :
The details of the vulnerability must include :

1. Basic information

The complete vulnerability exploitation process, associated URLs, screenshots, code and POC. If it does not comply with the rules, the vulnerability may not pass the examination.

2. IoT vulnerabilities must also provide :

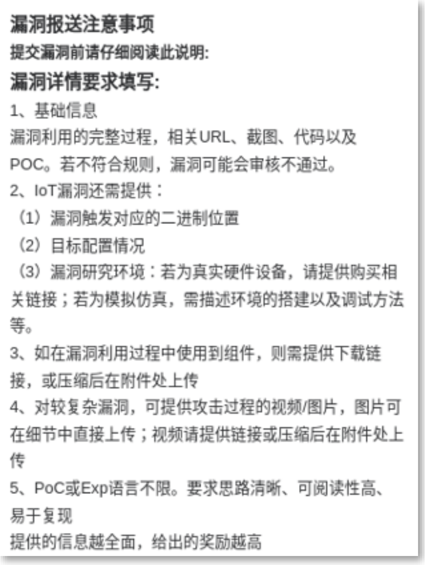
- *The binary location corresponding to the vulnerability trigger*
- *Target configuration*
- *Vulnerability research environment :*
  - *If this is a genuine hardware device, please provide the relevant purchase links;*
  - *If this is a simulation, please describe the methods used to build and debug the environment, etc.*

3. If a component is used in the process of exploiting the vulnerability, a download link must be provided, or the component must be compressed and downloaded in the attachment.

4. For more complex vulnerabilities, videos/images of the attack process can be provided. Images can be downloaded directly from the details; please provide a link or compress the video and upload it as an attachment.

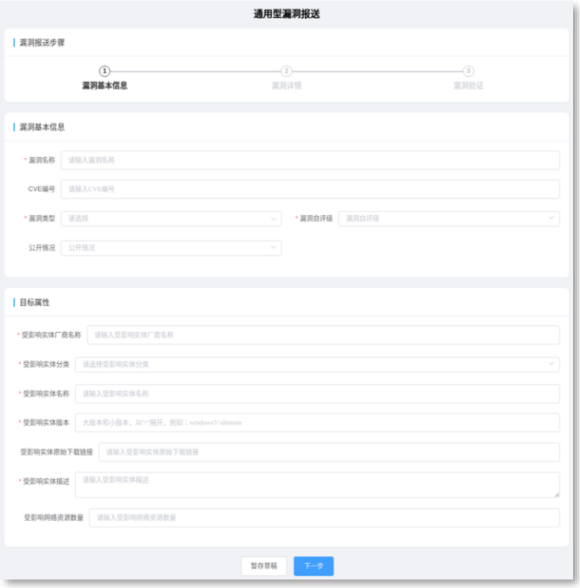
5. There is no limit to the POC or EXP language. Requires clear thinking, high clarity and easy reproduction.

The more complete the information provided, the higher the reward will be. »



漏洞报送注意事项
提交漏洞前请仔细阅读此说明:
漏洞详情要求填写:
1、基础信息
漏洞利用的完整过程，相关URL、截图、代码以及POC。若不符合规则，漏洞可能会审核不通过。
2、IoT漏洞还需提供：
（1）漏洞触发对应的二进制位置
（2）目标配置情况
（3）漏洞研究环境：若为真实硬件设备，请提供购买相关链接；若为模拟仿真，需描述环境的搭建以及调试方法等。
3、如在漏洞利用过程中使用到组件，则需提供下载链接，或压缩后在附件处上传
4、对较复杂漏洞，可提供攻击过程的视频/图片，图片可在细节中直接上传；视频请提供链接或压缩后在附件处上传
5、PoC或Exp语言不限。要求思路清晰、可阅读性高、易于复现
提供的信息越全面，给出的奖励越高

Figure 3 : Translation of the CNNVD guidelines relating to the vulnerability information submitted



通用型漏洞报送

漏洞报送步骤

① 漏洞基本信息 ② 漏洞详情 ③ 漏洞验证

漏洞基本信息

* 漏洞名称	请输入漏洞名称
CVE编号	请输入CVE编号
* 漏洞类型	请选择
* 漏洞自评级	漏洞自评级
公开情况	公开情况

目标属性

* 受影响实体厂商名称	请输入受影响实体厂商名称
* 受影响实体分类	请选择受影响实体分类
* 受影响实体名称	请输入受影响实体名称
* 受影响实体版本	大版本和小版本，以"/"隔开，例如：windows7/ ultimate
受影响实体原始下载链接	请输入受影响实体原始下载链接
* 受影响实体描述	请输入受影响实体描述
受影响网络资源数量	请输入受影响网络资源数量

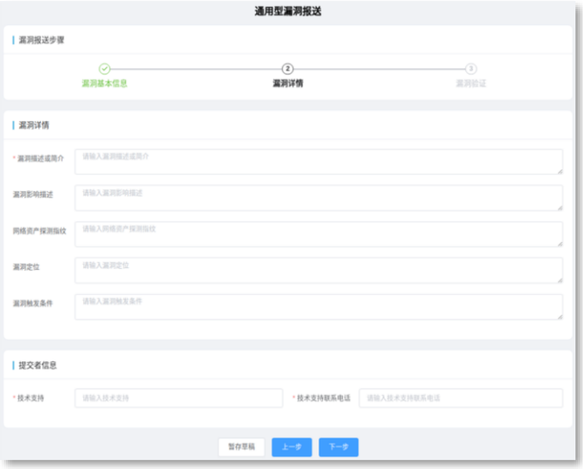
« **Basic information on vulnerability**

- * Name of vulnerability
- CVE number
- * Type of vulnerability
- Divulgation
- * Self-assessment of vulnerability

Targe attribute

- * Name of the manufacturer of the entity concerned
- * Classification of entities concerned
- * Name of the entity concerned
- * Version of the entity concerned
- Original download link for the entities concerned
- * Description of the entities concerned »

Figure 4 : Translation of the first page of the submission form



通用型漏洞报送

漏洞报送步骤

✓ 漏洞基本信息 ② 漏洞详情 ③ 漏洞验证

漏洞详情

* 漏洞描述或简介	请输入漏洞描述或简介
漏洞影响描述	请输入漏洞影响描述
网络资产探测指纹	请输入网络资产探测指纹
漏洞定位	请输入漏洞定位
漏洞触发条件	请输入漏洞触发条件

提交者信息

* 技术支持	请输入技术支持
* 技术支持联系电话	请输入技术支持联系电话

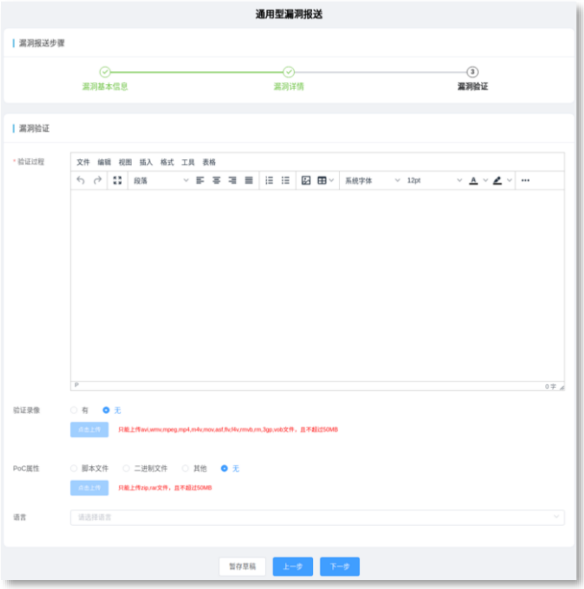
« **Details of the vulnerability**

- * Description or introduction of the vulnerability
- Description of the impact of the vulnerability
- Network traffic footprint
- Location of the vulnerability
- Conditions triggering the vulnerability

Information about the issuer

- * Technical support
- * Technical support contact number »

Figure 5 : Translation of the second page of the submission form



通用型漏洞报送

漏洞报送步骤

漏洞基本信息 → 漏洞详情 → ③ 漏洞验证

漏洞验证

* 验证过程

验证录像 ○ 有 ● 无

只能上传avi,wmv,mpeg,mp4,m4v,mov,asf,flv,f4v,rmvb,rm,3gp,vob文件，且不超过50MB

PoC属性 ○ 脚本文件 ○ 二进制文件 ○ 其他 ● 无

只能上传zip,rar文件，且不超过50MB

语言 请选择语言

« Checking for vulnerabilities

- * Verification process
- Video
- Proof-Of-Concept (POC)
- Language »

Figure 6 : Translation of the last page of the submission form

The items preceded by an asterisk (*) must be provided prior to submission :

The name of the vulnerability;
The type of vulnerability;

- *Code issues*
    - *Authorization issues*
        - *Permissions and access control issues*
        - *Trust management issues*
    - *Race condition issue*
    - *Handle logic errors*
    - *Wrong number*
    - *undeclared issue*
    - *Encryption issues*
    - *Data conversion issues*
    - *Resource management errors*
    - *Input validation error*
        - *Cross-site request forgery*
        - *Buffer error*
        - *Backlink*
        - *Injection*
            - *Code injection*
            - *Cross-site scripting*
            - *Command injection*
            - *Format string error*
            - *SQL injection*
        - *Path traversal*
- *Configuration error*
- *Others*
- *Environmental issues*
    - *Fault injection*
    - *Information leakage*
        - *Log information leakage*
        - *Debugging information leakage*
        - *Side channel information leakage*

Self-assessment of vulnerability;

- Extremely dangerous
- High risk
- Medium risk
- Low risk

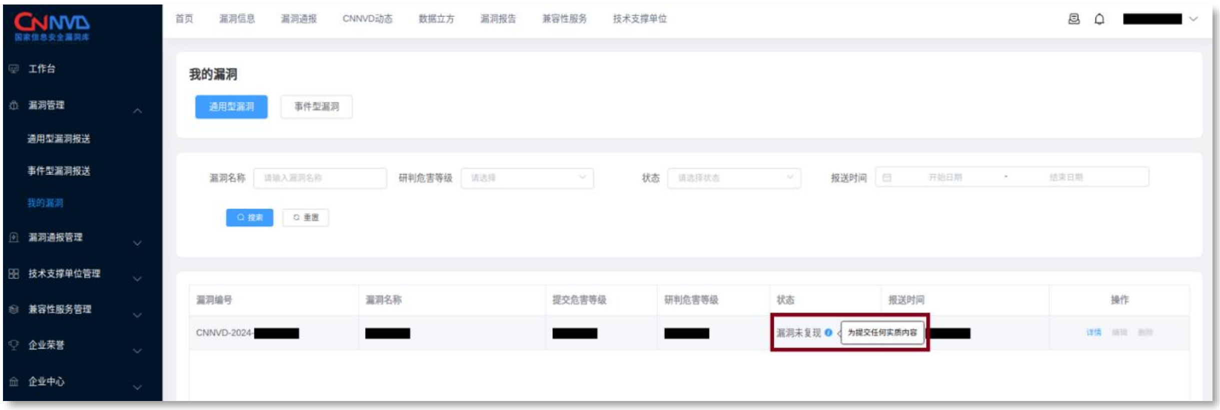
The classification of the entities concerned;
The name of the entity concerned;

- *Browser*
- *Office Software*
- *Database*
- *web application*
- *Website building system*
- *operating system*
- *Image processing software*
- *OA system*
- *PDF editor, reader*
- *Major email sites*
- *Email server*
- *email client*
- *compressing software*
- *Video player software*
- *Web plug-in*
- *Website building system*
- *antivirus software*
- *driver*
- *Industrial control equipment*
- *Printer*
- *social application*
- *Industrial control software*
- *Internet equipment*
- *safety equipment*
- *Operator core network element equipment*
- *APP*
- *Virtualization platform*
- *security system*
- *System Tool*
- *Other software*
- *Middleware*
- *other*

Description of the entities concerned;
Description of the vulnerability;
Details of the informer;
The verification process

Once the vulnerability has been submitted to the CNNVD, the company's user interface provides an overview showing the status of the verification of the information provided. CNNVD operators can study the vulnerability in question and inform us, in less than 24 hours, whether it has been successfully reproduced or not.

This approach by the Chinese government - combined with the attempt to reproduce the vulnerability submitted - confirms the supposedly malicious purpose of this database. Such a practice would be totally unthinkable on Western platforms, and even less in the United States with its NVD, which adopts a non-intrusive, non-coercive methodology.



[redacted]

我的漏洞

漏洞名称 请输入漏洞名称 研判危害等级 请选择 状态 请选择状态 报送时间 开始日期 - 结束日期

漏洞编号	漏洞名称	提交危害等级	研判危害等级	状态	报送时间	操作
CNNVD-2024-[redacted]	[redacted]	[redacted]	[redacted]	漏洞未复现 为提交任何实质内容	[redacted]	详情 编辑 删除

Figure 7 : User interface for showing the status of submitted vulnerabilities

V. The measured impact of the regulation relating to the management of security vulnerabilities

A simple statistical analysis of the two Chinese databases - CNVD and CNNVD - enabled us to see the real impact of this regulation. The CNVD provided us with an insight into its impact, as we noted a drastic fall in the number of vulnerability submissions. This can be explained by the fact that CNVD users are obliged to publish on the government database.

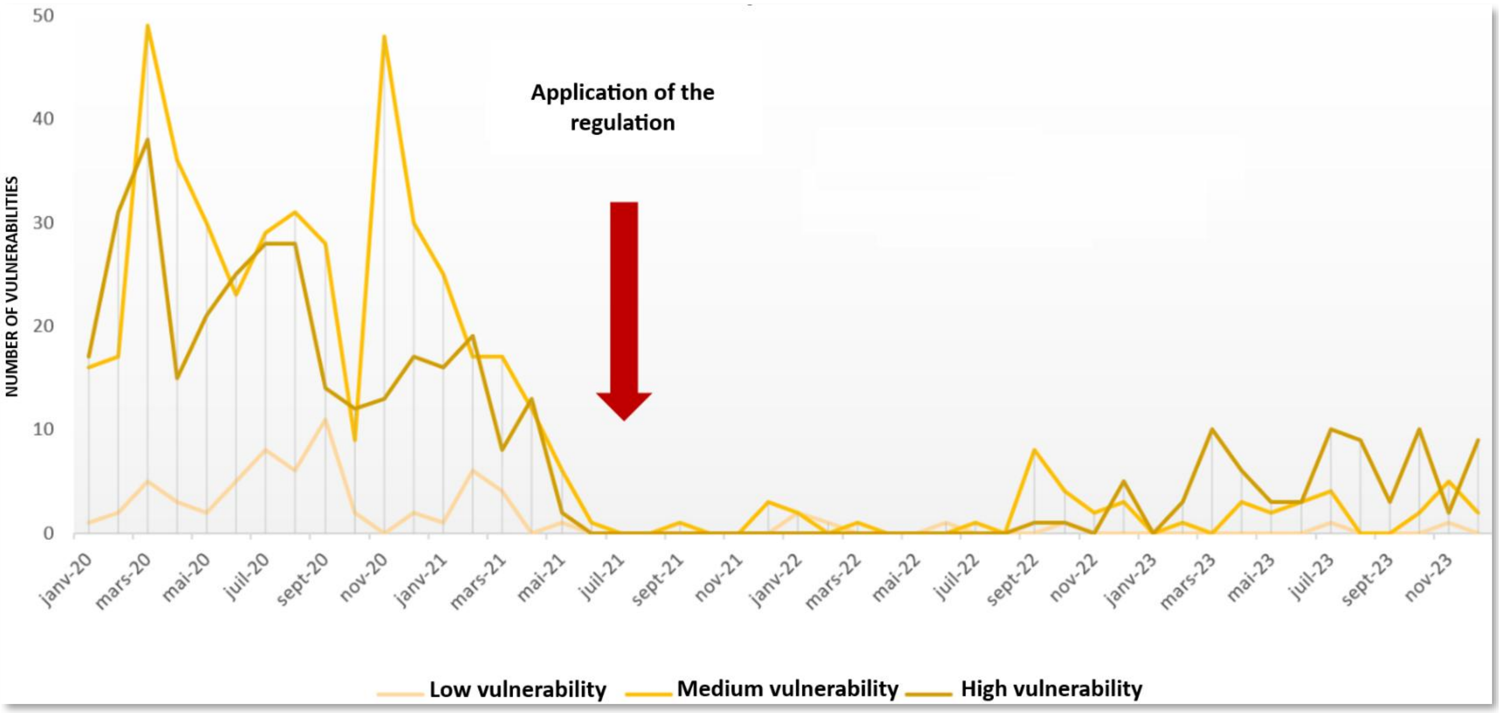
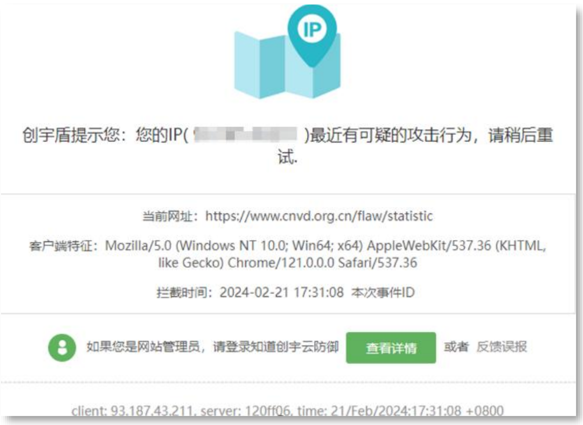


Figure 8 : Statistics on vulnerabilities submitted to the "Industrial Control System" (CNVD sub database)

On the contrary, the CNNVD will show resistance to its analysis, through what appears to be a deliberate and controlled obfuscation of its statistical data (e.g. false 404 errors; IP blocking; etc.).



创宇盾提示您：您的IP([redacted])最近有可疑的攻击行为，请稍后重试.

当前网址：https://www.cnvd.org.cn/flaw/statistic

客户端特征：Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

拦截时间：2024-02-21 17:31:08 本次事件ID

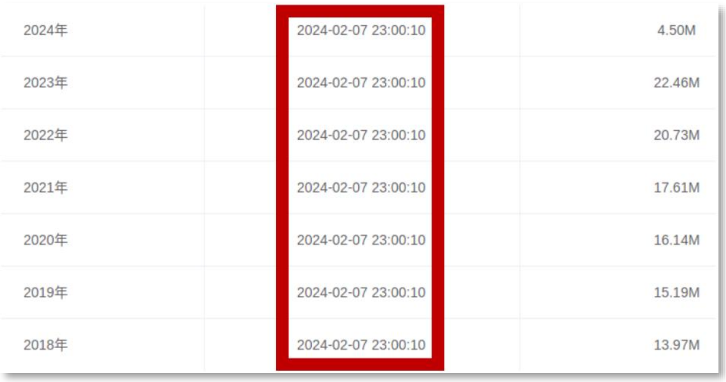
如果您是网站管理员，请登录知道创宇云防御

client: 93.187.43.211, server: 120ff06, time: 21/Feb/2024:17:31:08 +0800

Figure 9 : « TranShiels tells you that your IP (xx.xxx.xx.xxx) has recently been subject to a suspicious attack, please try again later »

Figure 10 : « Error 404 »

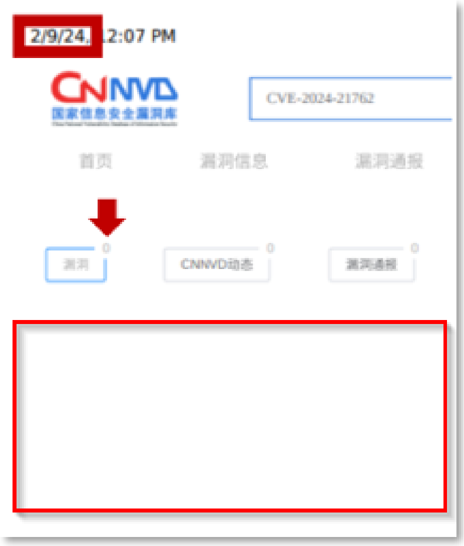
Nevertheless, we were able to highlight two interesting aspects of the CNITSEC database. The first concerns the daily updating of all its backups of the platform, even those dating back several years.



2024年	2024-02-07 23:00:10	4.50M
2023年	2024-02-07 23:00:10	22.46M
2022年	2024-02-07 23:00:10	20.73M
2021年	2024-02-07 23:00:10	17.61M
2020年	2024-02-07 23:00:10	16.14M
2019年	2024-02-07 23:00:10	15.19M
2018年	2024-02-07 23:00:10	13.97M

Figure 11 : Capture d’écran du 08.02.2024

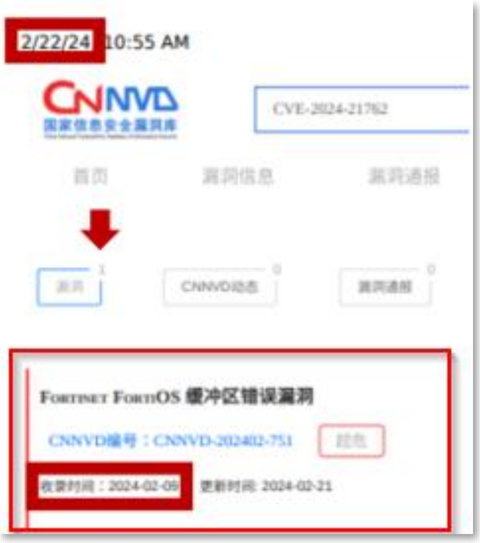
By monitoring the US NVD over several days, we were able to detect the appearance of a critical vulnerability (CVE-2024-21762) reported on 9 February 2024 by the company FortiGuard. Representative of a lack of reliability, we were able to note that it took more than thirteen days for this vulnerability to appear publicly in the CNNVD. What's more, it would appear that the publication date was obviously falsified by backdating in order to be identical to the date of publication on the NVD.



2/9/24, 12:07 PM

CVE-2024-21762

Figure 12 : Screenshot from 2024.02.09



2/22/24 10:55 AM

CVE-2024-21762

Fortinet FortiOS 缓冲区错误漏洞

CNNVD编号：CNNVD-202402-751 超危

收录时间：2024-02-09 更新时间: 2024-02-21

Figure 13 : Screenshot from 2024.02.22

During an attack, unauthenticated actors can use this critical vulnerability to execute arbitrary code or commands via the Fortinet application, thereby seriously exposing its users' data and infrastructure. Looking at the vulnerability submission process carried out previously, it is impossible to explain this time lag by a possible platform management flaw.

The most plausible hypothesis would be that the information concerning this vulnerability was deliberately not made public in order to allow Chinese intrusion sets to exploit it. It seems that this approach is not recent and that it existed prior to the publication of the RMSV, sometimes with delays of several tens of days.

VI. A regulation with a relativised impact

It should be noted that the influence of the regulation can be relativised by the companies themselves. The way entities interpret the RMSV differs, as do the risks they are prepared to take to avoid disclosing their vulnerabilities. While some will strictly comply with the legislation and requirements of the Chinese authorities - with the aim of preserving their economic assets and avoiding sanctions - other, more important companies (e.g. the GAFAMs) have probably developed strategies to avoid being submerged by them (e.g. correcting the vulnerability without reporting; incomplete information communicated; etc.). In addition, the economic impact of these large companies would prevent any economic pressure from the Chinese government. It is undeniable that this regulation facilitates the detection of vulnerabilities, but in the end it is not as extensive as we might think.

Conclusion

In July 2023, a book entitled "General Secretary Xi Jinping's Introduction to Important Ideology Regarding China as Cyber Powerhouse" was published by the Cyberspace Administration of China (CAC). It was analysed by cybersecurity researcher Dakota Cary, who managed to obtain this discreet, limited and resource-rich document. In it, the Chinese Communist Party sets out its visions for the future of the internet, both inside and outside of its territory and firewall.

Chapter 5 of the book is devoted specifically to cyber security policy, highlighting the importance **of an integrated and collaborative approach to ensuring national security**. This mirrors and puts into perspective our previous analysis.

According to the PRC, **IT security plays an essential role in national stability**. Moreover, it would have an impact on critical sectors such as politics, the economy, energy and telecommunications. Without robust cyber security, the whole society would be at risk. **Technological advances such as artificial intelligence and 5G have also increased data security risks**, according to the Chinese government. Moreover, the fact that some countries are militarising cyberspace would drastically increase the risk of cyber conflicts, posing new challenges to stability and world peace.

China has therefore clearly indicated that it wants to **defend its population and its territory against the threats posed by the development of technology** and *de facto* digital means of aggression. It is highlighting **the weaponisation of digital space by foreign powers**, which is paradoxical given the large number of Chinese intrusion sets identified for spying on foreign countries on behalf of the Chinese government (cf. i-SOON analysis carried out by Intrinsec's CTI team). **Collecting information on cybersecurity incidents** is therefore an essential step in establishing the vision provided by the CAC, which would then be the public justification for the real strategy emanating from the CNNVD.

This work also highlights the actions underway to **reform education in cybersecurity and to train more individuals in defence and offensive actions**. In addition, it highlights the importance **of integration in cybersecurity** to increase national capacity to adapt to evolving threats. This makes it easier to understand China's strategy of using the intrusion sets present on its territory to maintain this objective. This integration would make it possible to **"protect" critical infrastructures** more effectively, while ensuring that protection systems are perfectly integrated and coordinated.

When China states that - in order to respond quickly and effectively to cyber attacks - it is essential to **improve the mechanisms of detection, coordination and response to security incidents**, it argues that it is necessary to **develop legal and technical measures** with the aim of "protecting" its citizens. Other texts - restrictive and liberticidal - such as the RMSV, could emerge in the next few years to better achieve this objective. However, combined with **the liabilities and capabilities of the PRC and its satellite entities**, it is more appropriate to say that the development of these means and resources - particularly legal ones - will rather **serve the appetite of Chinese intelligence, and be detrimental to its nationals as well as to the international society**.

Sources

- https://geoconfluences.ens-lyon.fr/glossaire/gafa-gafam
- http://www.recordedfuture.com/blog/chinese-vulnerability-data-altered
- http://www.theregister.com/2024/03/18/more_than_133000_fortinet_appliances/
- https://cve.mitre.org/cve/list_rules_and_guidance/cve_assignment_information_format.html
- https://cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/
- https://www.securityweek.com/2-5-million-offered-at-upcoming-matrix-cup-chinese-hacking-contest/
- https://www.oodaloop.com/archive/2022/01/13/the-tianfu-cup-ios-poc-exploits-and-the-future-of-global-hacker-competitions/
- https://techjournalism.medium.com/how-to-automate-leak-data-osint-verification-i-soon-1a0a81744e7b
- https://en.wikipedia.org/wiki/2022_Winter_Olympics
- https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
- https://nvd.nist.gov/
- https://www.numerique.gouv.fr/actualites/le-bug-bounty-un-dispositif-innovant-pour-renforcer-la-securite-des-services-numeriques/
- https://www.gchq.gov.uk/news/cyberuk-2024
- https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=4&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all/&
- http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm
- http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm
- https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf
- https://mp.weixin.qq.com/s/ErW6mF01DaRl5cJDwsPjDQ?scene=25
- http://www.cac.gov.cn/2016-11/07/c_1119867116.htm
- https://www.fortinet.com/fr/resources/cyberglossary/man-in-the-middle-attack
- https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/
- http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/13/content_1384075.htm
- https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html
- https://interpret.csis.org/translations/general-secretary-xi-jinpings-introduction-to-important-ideology-regarding-china-as-a-cyber-powerhouse-chapter-5-building-a-durable-national-cybersecurity-barrier/
- http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/05/content_1381903.htm
- https://www.portail-ie.fr/univers/droit-et-intelligence-juridique/2024/droit-et-strategie-comprendre-lart-du-lawfare/
- https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived
- https://www.latimes.com/la-fi-spam11may11001420-story.html