SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

俄乌冲突

全球网络战预演？

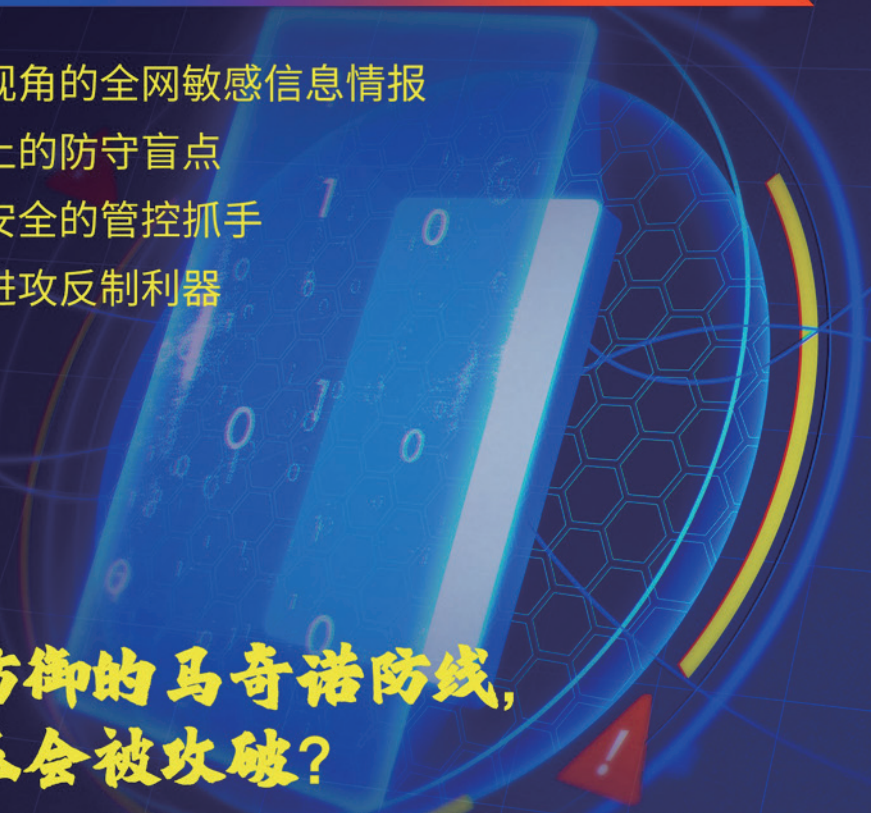
P10

第15期
2022 年 3 月

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器



纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

网络战不可预知的未来

俄罗斯与乌克兰的战争表明，网络攻击已成为现代战争“先发制人的武器”。

在俄罗斯军队行动之前，针对乌克兰的网络攻击就已经开始：从虚假宣传活动到数据窃取泄露，从擦除数据和破坏系统的恶意擦除软件到大规模分布式拒绝服务 (DDoS) 攻击。

目前俄乌间的网络战正以专家没有预料到的方式进行。俄乌之间的网络攻击导致双方的大量政府网站、金融与电信服务受到影响。2 月 24 日，针对欧洲卫星运营商 Viasat 的攻击中断了乌克兰的互联网接入，从而不得不求助于马斯克的星链服务，攻击还导致数千台使用 Viasat 通信的德国风力涡轮机瘫痪。

与俄罗斯的网络攻击能力相比，目前网络攻击的影响仍微乎其微，这可能是俄罗斯不想破坏其认为可以迅速接管的系统。正如安全人员的研究，网络攻击不仅能够导致电网等系统关闭，甚至可能会导致爆炸或损坏，从而影响在严酷的天气中的居民生活。2021 年，黑客组织对美国石油管道公司的攻击已验证了这一点。

鉴于西方联合起来支持乌克兰，双方网络战的范围可能很广泛，有黑客组织威胁，将攻击与俄罗斯为敌的国家和企业。对于俄罗斯来说，与乌克兰的战争很可能成为其下一代网络武器的试验场。释放网络武器所造成的破坏远远超出最初设定的目标。由于网络攻击的这一溢出效应，最终也有可能演变成大规模的全球性网络冲突。最坏的情况或许尚未到来，很难预测接下来会发生什么，以及未来的网络战将以何种方式进行，将造成什么样的影响。

核试验时代可能已经结束，但网络战时代才刚刚开始。严重的网络攻击可能会产生与自然灾害类似的影响，破坏重要基础设施并引发连锁危机。

面对对手已经在关键基础设施网络中站稳脚跟的可能性，我们必须时刻为各种网络攻击的未知和可能性做好准备，尽一切可能将攻击者入侵时的潜在损害降到最低。

这注定是一场没有终点的马拉松，任何的倦怠都可能加剧现有的问题， 带来巨大的危险。

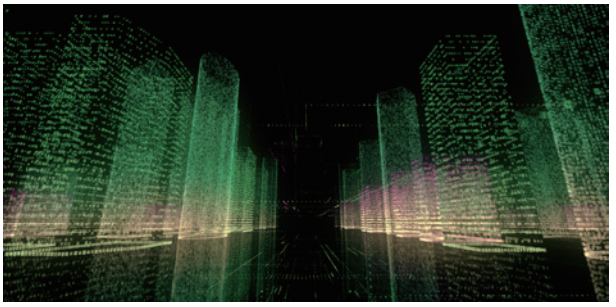
总编辑

李建平

2022 年 3 月 1 日

CONTEN

目录



安全态势

P4 | 俄乌冲突引发网空混战，关基成网络攻击重点

P4 | 以色列遭遇大规模网络攻击，多个重要政府网站瘫痪 1 小时

P5 | 俄乌冲突网络风险外溢？网络攻击导致数万名卫星用户断网

P5 | Conti 勒索软件内部数据全泄露：俄乌冲突引发网络武器库失控

P6 | Kubernetes CRI-O 引擎任意代码执行漏洞安全公告

P6 | OpenSSL 拒绝服务漏洞 (CVE-2022-0778) 安全风险通告

P7 | Windows Remote Desktop Client 远程代码执行漏洞安全风险通告

P7 | Linux 内核权限提升漏洞（CVE-2022-25636）安全风险通告

P8 | 《移动互联网安全审计指南》等 4 项网络安全国家标准获批发布

P8 | 网信办《未成年人网络保护条例》再次公开征求意见

P8 | 国家药监局发布《医疗器械网络安全注册审查指导原则 (2022 年修订版)》

P9 | 国务院 2022 年政府工作报告：强化网络安全、数据安全和个人信息保护

P9 | 美国通过《2022 年关键基础设施网络事件报告法案》

月度专题

俄乌冲突：全球网络战预演？

P10

俄乌的网络战以专家未预料到的方式进行，将网络武器与其他传统战争工具结合在一起，推动混合战进入新阶段。未来网络战或将成为战争胜负的关键，俄乌冲突中的全球黑客大战，或许是全球网络战的预演。

TS

攻防一线

P26

漏洞情报：
为什么、要什么和怎么做

安全之道

P32

守护百年协和金字招牌
天眼打造“智慧医疗”安全标杆

奇安信人

P36

初心如炬，永不灭

P42

她们 | 冬奥背后的“奇女子”
诠释新时代的“女性力量”

安全叨客

P48

听说周报写 5000 字
就能升职加薪？不存在的！

奇安资讯

P51 | 奇安信圆满完成北京冬奥会与冬残奥会网络安全保障任务
P51 | 冬奥“零事故”经验宣讲团成立大会召开
P52 | 奇安信集团副总裁韩争光受聘为工联众测平台特邀专家
P52 | 北京市委统战部部长游钧一行到访奇安信调研冬奥网络安全保障工作
P53 | 奇安信发布 2021 漏洞态势报告：重点漏洞数量急剧上涨
P53 | 北京 2022 年冬奥会网络安全“零事故”经验总结研讨会在奇安信召开
P54 | 独家披露！奇安信发布针对乌克兰目标的系统破坏攻击分析
P54 | 北京奇安盘古实验室发布报告 揭露美国安局顶级后门“电幕行动”
P55 | 奇安信与人保财险合作案例入选网络安全保险新业态新模式十大典型案例
P55 | 奇安信斩获 CSA 2021 安全磐石奖 彰显全栈云安全能力
P56 | 实力领先！奇安信安全访问服务（Q-SASE）斩获金智奖
P56 | 奇安信荣获 CNVD 漏洞信息报送突出贡献单位等多项荣誉

第 15 期
《网安 26 号院》编辑部
主办 奇安信集团

总　　编　　辑：李建平
副　　总　　编：裴智勇
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
安全叨客主编：王梦琪
奇安资讯主编：陈　冲

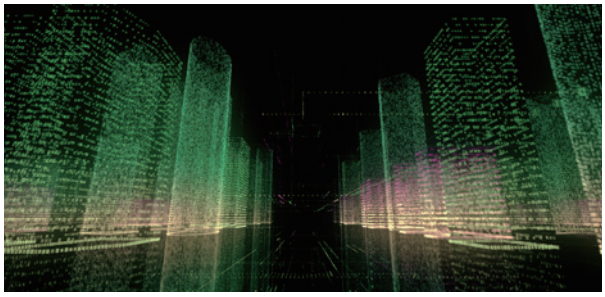
奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载
索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2021-L0058 号
印刷数量：45000 本
印刷单位：北京七彩虹印刷有限公司
下载地址：www.qianxin.com

事件篇

俄乌冲突引发网络空间混战，俄乌两国的关基设施密集遭受网络攻击，被迫中断服务。冲突风险还外溢至我国，有境外组织劫持国内计算机资源，对俄乌等国进行网络攻击。



俄乌冲突引发网空混战，关基成网络攻击重点

综合消息，自 2 月 24 日起，俄乌冲突全面爆发，引发了网络空间的混战，从国家网军、乌克兰地下黑客、俄罗斯民间“网络卫士”到勒索软件组织、国际黑客组织，各方势力轮番上场。截至 3 月 12 日，据统计有 65 个黑客组织参与行动。俄乌两国的政务、通信、金融等关基设施密集遭受网络攻击，被迫中断服务。混战还外溢至其他地区，如我国计算机资源被劫持攻击俄乌等国、美国卫星运营商中断服务等。

以色列遭遇大规模网络攻击，多个重要政府网站瘫痪 1 小时

据新华社 3 月 14 日消息，以色列多个政府网站遭到黑客攻击，短时间瘫痪。目前遭到攻击的各个网站已经恢复。遭到攻击的政府网站包括以色列总理府、内政部、司法部等。以色列网络指挥部发表声明说，一家以色列网络运营商“遭到拒绝服务攻击”，造成多个政府网站无法正常登录和使用。以色列网络指挥部已宣布进入紧急状态，以了解此次攻击造成的破坏程度，并对电力、供水等基础设施进行全面检查，了解是否同样遭到了攻击。

我国互联网遭受境外网络攻击：资源被滥用攻击俄乌等国

据新华社 3 月 11 日消息，国家互联网应急中心监测发现，2 月下旬以来，我国互联网持续遭受境外网络攻击，境外组织通过攻击控制我境内计算机，进而对俄罗斯、乌克兰、白俄罗斯进行网络攻击。经分析，这些攻击地址主要来自美国，仅来自纽约州的攻击地址就有 10 余个，攻击流量峰值达 36Gbps，87% 的攻击目标是俄罗斯，也有少量攻击地址来自德国、荷兰等国家。据悉，国家互联网应急中心已及时对以上攻击行为最大限度予以处置。

全球最大数字报纸发行平台遭到网络攻击，被迫关闭多天

据 ZDNet 3 月 8 日消息，全球最大的数字报纸与杂志发行平台之一 PressReader 遭遇网络攻击，平台关闭约 4 天时间，导致读者无法访问出版物。PressReader 平台收录了世界各地 7000 多种刊物，客户包括报纸、图书馆及博物馆等多个领域，还有一些客户把 PressReader 作为唯一电子发行平台。

PressReader 声称自己并未唯一的受害者。过去几周内，曾经出现一波针对北美多家企业的大规模“安全事件”，其受到的攻击只是其中一例。

俄乌冲突网络风险外溢？网络攻击导致数万名卫星用户断网

据法新社 3 月 4 日消息，2 月 24 日俄乌冲突爆发时，覆盖乌克兰地区的美国卫星运营商 Viasat 遭遇网络事件，导致欧洲多家依托 Viasat 的卫星互联网运营商的部分网络中断服务，数万名卫星网络用户断网。法国太空司令部司令 Michel Friedling 将军称，Viasat 民用网络遭遇了网络攻击，导致数以万计的终端在攻击之下失去用处。

Conti 勒索软件内部数据全泄露：俄乌冲突引发网络武器库失控

据 Threatpost 3 月 2 日消息，俄乌冲突引发民间网络安全能力者的分裂，Conti 勒索软件选择站队俄罗斯，引发一名乌克兰安全研究人员的愤怒，开始疯狂地公开泄露 Conti 内部数据。据分析，泄露数据包括 Conti 勒索软件代码、TrickBot 木马代码、Conti 培训材料、Conti/TrickBot 内部交流的各种攻击技巧等，已然是一个小型网络武器库。这些泄露数据可谓双刃剑，安全研究人员可以了解 Conti 的策略、代码开发、货币化方式、潜在成员身份等信息，采取更可靠的防御手段；恶意软件开发者也可以利用这批数据，指导开发更多类似 TrickBot 的恶意软件。

BlackMoon 僵尸网络在国内大规模传播，已感染数百万终端

据 CNCERT 3 月 1 日消息，国家互联网应急中心（CNCERT）监测发现，BlackMoon 僵尸网络在互联网上进行大规模传播，通过跟踪监测发现其 1 月控制规模（以 IP 数计算）已超过 100 万，日上线肉鸡数最高达 21 万，给网络空间带来较大威胁。BlackMoon 僵尸网络位于境内肉鸡按省份统计，排名前三位的分别为广东省（12.7%）、河南省（9.3%）和江苏省（7.6%）；按运营商统计，电信占 57.5%，联通占 22.9%，移动占 19.4%。

英伟达 1TB 内部敏感数据失窃，遭黑客团伙“花式”勒索

据 BleepingComputer 3 月 1 日消息，国际芯片巨头英伟达确认，在 2 月 23 日遭到网络攻击，导致部分专有数据和员工登录数据泄露。此前，Lapsus$ 黑客团伙连续一周公开发布此次黑客攻击的细节，以泄露敏感数据为由来勒索英伟达，要求解锁挖矿限制、开源显卡驱动等。勒索未果的情况下，Lapsus$ 放出了部分敏感数据。值得一提的是，Lapsus$ 入侵英伟达内部网络后，英伟达进行反击加密了他们窃取的数据，但他们留有备份，使得这次反击未能成功。

关键供应商被黑，丰田汽车无奈关停日本所有工厂

据 BleepingComputer 2 月 28 日消息，由于网络攻击导致关键供应商小岛工业出现系统故障，丰田公司被迫宣布，暂停日本 14 家工厂的 28 条生产线。这将令丰田公司月减产约 13000 辆汽车。这是又一起制造巨头因网络攻击被迫停产。丰田公司一直以“准时制”精益制造法的超级高效著称，但这在当下已然成为软肋，没有安全保障能力，其所接入的网络环境或许随时会被恶意攻击倾覆。

漏洞篇

近期，OpenSSL、Linux 内核、Windows 远程桌面客户端等多个全球基础软件漏洞的利用代码公开泄露，已构成现实威胁，建议用户尽快自查并更新修复。

Kubernetes CRI-O 引擎任意代码执行漏洞安全公告

3 月 18 日，美国网络安全与基础设施安全局发布安全公告，CRI-O 发布安全更新，修复 1.19 版本的一个严重漏洞（CVE-2022-0811）。CRI-O 是 Kubernetes 的容器运行时引擎，可以替代 Docker。本地攻击者可以利用此漏洞，控制受影响的 Kubernetes 环境及使用 CRI-O 容器运行时的其他软件或平台。目前，CRI-O v1.19.6、v1.20.7、v1.21.6 等新版本已修复漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

OpenSSL 拒绝服务漏洞（CVE-2022-0778）安全风险通告

3 月 17 日，奇安信 CERT 监测到 OpenSSL 官方发布安全更新，修复了 OpenSSL 拒绝服务漏洞（CVE-2022-0778）。OpenSSL 的 BN_mod_sqrt() 函数包含一个致命错误，攻击者可以通过构造特定证书来触发无限循环，由于证书解析发生在证书签名验证之前，因此任何解析外部提供的证书场景都可能实现拒绝服务攻击。目前，此漏洞细节及 PoC 已公开，经奇安信 CERT 验证， PoC 有效且稳定。鉴于此漏洞影响范围极大，建议客户尽快做好自查及防护。

Linux kernel 安全漏洞（CVE-2022-0847）预警

3 月 11 日，国家信息安全漏洞库收到关于 Linux kernel 安全漏洞（CNNVD-202203-522、CVE-2022-0847）情况的报送。成功利用此漏洞的攻击者，可提升本地用户权限。LinuxKernel 5.8-5.16.11、5.8-5.15.25、5.8-5.10.102 等版本均受此漏洞影响。目前，Linux 官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

APC Smart-UPS 设备多个高危漏洞安全风险通告

3 月 11 日，奇安信 CERT 监测到 APC Smart-UPS 设备中多个高危漏洞，这些漏洞统称为 "TLStorm" 漏洞。漏洞编号分别为 CVE-2022-22805、CVE-2022-22806 和 CVE-2022-0715。CVE-2022-22805 与 TLS 相关，主要是数据包重组引发的缓冲区溢出，可能导致远程代码执行；CVE-2022-22806 主要是 TLS 握手中存在状态混淆，导致身份验证绕过；CVE-2022-0715 属于系统设计缺陷，受影响设备上的固件更新未以安全方式进行加密签名，意味着攻击者可

以制作恶意固件并使用各种路径进行安装，可能导致远程代码执行。鉴于这些漏洞影响范围极大，建议客户尽快做好自查及防护。

Windows Remote Desktop Client 远程代码执行漏洞安全风险通告

3 月 9 日，奇安信 CERT 监测到微软发布月度安全更新，其中包括 Windows Remote Desktop Client 远程代码执行漏洞 (CVE-2022-21990)。要利用此漏洞，攻击者需要控制远程桌面服务器，然后诱导用户连接到该服务器，如利用社会工程学、DNS 中毒、中间人攻击、破坏合法服务器等方式。当受害者使用易受攻击的远程桌面客户端连接到攻击服务器时，攻击者可以在 RDP 客户端计算机上触发远程代码执行。目前，此漏洞 PoC 已在互联网公开，经奇安信 CERT 验证，此 PoC 有效，黑客可在此 PoC 的基础上开发出完整的漏洞利用，现实威胁进一步上升。鉴于该漏洞影响较大，建议用户尽快更新。

Linux 内核权限提升漏洞（CVE-2022-25636）安全风险通告

3 月 8 日，奇安信 CERT 监测到 Linux 内核权限提升漏洞 (CVE-2022-25636)，具有用户账户的本地攻击者可利用此漏洞，获得对越界内存的访问权限，从而实现从普通权限用户身份提升到 ROOT 权限，或导致系统崩溃。目前，此漏洞细节、PoC 及 EXP 已公开，经奇安信 CERT 验证，此漏洞 EXP 有效且稳定。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

PTC Axeda 代理和桌面服务器“Access:7”系列漏洞安全公告

3 月 8 日，美国网络安全与基础设施安全局发布工业控制系统咨询文件，详细说明了影响 PTC Axeda 代理和桌面服务器的一系列安全漏洞“Access:7”。成功利用这组漏洞，可导致完全系统访问、远程代码执行、读取 / 更改配置、访问读取文件系统、访问日志信息或拒绝服务等。PTC 是国际工业物联网数字化重要供应商，Axeda 平台是基于云的物联网平台。目前，PTC 官方已发布新版本修复了漏洞，建议用户尽快采取修复措施。

Clash 远程代码执行漏洞安全风险通告

2 月 25 日，奇安信 CERT 监测到流行跨平台代理软件核心程序 Clash 官方发布安全更新，修复低版本中存在的 Clash 远程代码执行漏洞。Clash 是一个基于规则的流行跨平台代理软件核心程序。攻击者可通过加载配置文件的方式，在 proxies 名称中插入恶意 JS 代码，最终导致远程代码执行。利用该漏洞需交互，用户需加载恶意 YAML 配置文件。目前漏洞利用细节及 PoC 已经公开，同时已在 Clash 0.19.8、0.19.4、0.18.8、0.17.2 版本上成功复现。鉴于该漏洞影响较大，建议用户及时更新至修复版本。

PostgreSQL JDBC Driver 多个漏洞安全风险通告

2 月 25 日，奇安信 CERT 监测到 PostgreSQL JDBC Driver 官方发布多个漏洞公告。其中包括 PostgreSQL JDBC Driver 任意代码执行漏洞 (CVE-2022-21724)：若受害机器可通外网，且 JDBC 连接 URL 属性可控，未经授权的远程攻击者可利用该漏洞执行任意代码；PostgreSQL JDBC Driver 任意文件写入漏洞 (QVD-2022-1479)：当连接 PostgreSQL 数据库的 URL 或参数 (loggerLevel、loggerFile) 可控时，即可写入任意文件。目前，漏洞利用细节及 PoC 均已公开，鉴于漏洞影响较大，建议用户及时更新。

政策篇

国内，国务院 2022 年政府工作报告发布，要求强化网络安全、数据安全和个人信息保护，为全年工作风向定下基调；

国际上，美国通过《2022 年关键基础设施网络事件报告法案》，要求关键基础设施所有者和运营者必须报告网络事件，或成为改变关基网络防护格局的关键点。

国内

《移动互联网安全审计指南》等 4 项网络安全国家标准获批发布

3 月 18 日，国信息安全标准化技术委员会发布公告称，4 项网络安全国家标准获批发布，将于今年 10 月 1 日生效。分别为：《信息安全技术 术语》（注：替代 2010 年版本）、《信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法》（注：替代 2006、2013 年版本）、《信息安全技术 重要工业控制系统网络安全防护导则》、《信息安全技术 移动互联网安全审计指南》。

网信办《未成年人网络保护条例》再次公开征求意见

3 月 14 日，国家互联网信息办公室就《未成年人网络保护条例（征求意见稿）》再次公开征求意见。征求意见稿共七章 67 条，涉及网络素养培育、网络信息内容规范、个人信息保护、网络沉迷防治等内容。在个人信息保护方面，征求意见稿提出，个人信息处理者处理未成年人敏感个人信息、确有必要向他人提供未成年人个人信息时，应在事前进行个人信息保护影响评估；每年对其处理未成年人个人信息是否遵守法律法规文件的情况进行合规审计。

国家药监局发布《医疗器械网络安全注册审查指导原则（2022 年修订版）》

3 月 9 日，国家药监局器审中心发布《医疗器械网络安全注册审查指导原则（2022 年修订版）》。《指导原则》是医疗器械网络安全的通用指导原则。《指导原则》从医疗器械电子接口、网络安全能力、网络安全验证与确认、网络安全可追溯分析、网络安全事件应急响应、网络安全更新等方面，提出了相应要求。《指导原则》要求，医疗数据通常属于重要数据，特别是敏感医疗数据含有个人信息，因此医疗数据出境应符合重要数据、个人信息、人类遗传资源信息出境安全评估相关规定；境外远程维护与升级若可访问医疗数据，也应符合医疗数据出境要求。

工信部印发《车联网网络安全和数据安全标准体系建设指南》

3 月 7 日，工信部宣布印发《车联网网络安全和数据安全标准体系建设指南》，聚焦车联网终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安

全保障与支撑等重点领域，着力增加基础通用、共性技术、试验方法、典型应用等产业急需标准的有效供给，覆盖车联网网络安全、数据安全的关键领域和关键环节。指南提出，到 2025 年，形成较为完善的车联网网络安全和数据安全标准体系。完成 100 项以上标准的研制。

国务院 2022 年政府工作报告：强化网络安全、数据安全和个人信息保护

3 月 5 日，国务院总理李克强向第十三届全国人民代表大会第五次会议作《2022 年政府工作报告》。报告提出，2022 年将推进国家安全体系和能力建设。强化网络安全、数据安全和个人信息保护。促进数字经济发展。加强数字中国建设整体布局。建设数字信息基础设施，逐步构建全国一体化大数据中心体系，推进 5G 规模化应用，促进产业数字化转型，发展智慧城市、数字乡村。加快发展工业互联网，培育壮大集成电路、人工智能等数字产业，提升关键软硬件技术创新和供给能力。完善数字经济治理，培育数据要素市场，释放数据要素潜力，提高应用能力，更好赋能经济发展、丰富人民生活。

美国通过《2022 年关键基础设施网络事件报告法案》

3 月 15 日，美国总统拜登签署《2022 财年综合拨款法案》（H.R.2471），其中 Y 部分为《2022 年关键基础设施网络事件报告法案》。该法案要求，16 个关基行业的关键基础设施所有者和运营者，应向美国网络安全与基础设施安全局（CISA）报告网络事件和勒索软件赎金支付消息，其中网络事件需在发生后 72 小时内报告，支付赎金需在发生后 24 小时内报告。这项制度还需要 CISA 后续发布规定来明确和落实，CISA 有 24 个月的时间制定规定。

美国 FCC 拟推动改进互联网基础协议安全

3 月 11 日，美国联邦通信委员会（FCC）在联邦公报上发布《安全互联网路由》文件，公开征集公众意见。这项草案希望解决边界网关协议（BGP）的主要安全漏洞，更好地保护各网络间传输的互联网流量。BGP 劫持漏洞除了可能影响邮件与网络流量，还可能令 VoIP 呼叫的完整性受损，并导致 911 应急服务及其他公共安全事务遭受破坏。FCC 希望了解，当前针对 BGP 的安全措施、是否有效、适用范围、阻碍电信运营商部署的障碍等情况。

俄罗斯联邦刑法修正案签署生效，严惩故意公开传播俄军虚假信息行为

3 月 4 日，俄罗斯总统普京签署俄罗斯联邦刑法修正案，规定公开故意发布有关俄罗斯武装部队虚假信息者，最高可判处三年监禁或 150 万卢布罚款。若利用其公职，出于雇佣关系，或基于政治、意识形态、种族、民族或宗教仇恨而违反有关法律，将处以最高 10 年的监禁或最高 500 万卢布的罚款。如果虚假信息造成严重后果，将判处 10 至 15 年监禁。

日本多部门发布公告，提请政府和关基运营者加强网络安全措施

3 月 1 日，日本经济产业省、金融厅、总务省等 7 部门联合发布公告，鉴于近期网络攻击的风险正在增加，并且有一家日本汽车零部件制造商当天宣布遭遇网络事件，在此呼吁政府机构和关键基础设施运营商，加深对网络威胁的认识，采取建议的安全措施加强防范，检测整个供应链并实施适当的安全措施，以便控制风险。此外，海外分支机构可能成为网络攻击日本关键系统的起点，请按照国内系统的同等标准实施安全措施。

专题主编　李建平

俄乌冲突：全球网络战预演？

俄乌的网络战以专家未预料到的方式进行，将网络武器与其他传统战争工具结合在一起，推动混合战进入新阶段。未来网络战或将成为战争胜负的关键，俄乌冲突中的全球黑客大战，或许是全球网络战的预演。

揭秘！俄乌网络战真实再现

作者 虎符智库特约作者 傅强

俄乌军事冲突的爆发成为全球关注的重大事件。在激烈的军事冲突的同时，一场平行的网络战正在进行。

这场战争以从未见过的方式将网络武器与其他传统战争工具结合在一起。鉴于俄乌网络攻击手段的介入，国际社会认为此次冲突是一次典型的“混合战争”（hybrid warfare）——混合了传统的军事行动，以及非传统的数字或网络战争。这或许验证了英国首相鲍里斯·约翰逊 2021 年的发言：“在欧洲大陆上进行大型坦克战的旧理念已终结。（支持传统战争的）网络战才是未来的战争方式。”

在战争前期、战争进行中、敌对各方、全球各个阵营中，网络攻击随处可见，通过网络空间传播虚假信息、释放信息烟幕、误导决策，以及通过网络攻击破坏重要基础设施和通信系统，网络攻击直接影响战争的进程，与传统的军事手段相互交织、互动推进。

目前，俄乌的数字战以网络战专家没有预料到的方式进行着：一方面是网络强国俄罗斯，在坦克越过边境前就开始了数字攻击。另一方面是在网络空间能力相对弱小的乌克兰，成为第一个通过公开招募国际黑客大军进行反击的国家。

这种虚拟空间攻击和物理攻击手段紧密结合、互相促动的模式，释放了现代战争的潜能，正在成为战争新形态。

一、俄乌网络战真实场景再现

新一轮俄乌冲突作为一个正在发生的现代版战争，为网络武器的运用提供了真实的场景分析环境。

网络战的几个主要手段，在本次冲突中也都能找到可以对号入座的行动案例。

（一）俄乌网络战的数轮攻击

据公开信息分析，截至目前可观察到的俄罗斯对乌克兰大规模、高水平的网络攻击有三波。

2022 年 1 月 14 日前后，第一轮攻击——WhisperGate 数据擦除软件。70 多个乌克兰政府网站遭到 APT 组织攻击，其中包括属于乌克兰外交部、教育部、能源部、国防部、国家紧急事务局、内阁等的中央和地区政府网站。乌克兰军事目标也受到越来越多的网络攻击和网络间谍活动的骚扰。上述攻击都包含着带有俄罗斯印记的高级持续威胁（APTs）。1 月 15 日，微软报告称发现 APT 组织向乌克兰的一些重要机构投递 WhisperGate 样本，相关样本的破坏行为会加密磁盘 MBR 和机器上指定类型的文件。

2 月 15 日前后，第二轮攻击——DDoS 攻击（拒绝服务攻击）。2 月 15 日，乌克兰多处信息资源遭到强大的 DDoS 攻击，导致 PrivatBank 和 OschadBank 的 Web 服务工作中断。国防部和乌克兰武装部队的网站也遭到攻击。2 月 18 日，乌克兰计算机应急响应小组（CERT-UA）在一份报告中表示，在这轮攻击中，攻击者曾动用到多种 DDoS 即服务平台，以及包括 Mirai 与 Meris 在内的多个僵尸网络。

美国政府已经认定这波 DDoS 攻击与俄罗斯武装部队总参谋部情报总局（GRU/ 格鲁乌）有关。美国国家安全副顾问 Anne Neuberger 表示，“我们已经掌握了俄情报总局与此次事件有关的技术信息，发现已知的 GRU 基础设施曾向乌克兰方面的 IP 地址和域名传输大量通信内容。”Neuberger 还补充道，尽管这些攻击“影

响有限”，但这也许是在“为更具破坏性的后续攻势奠定基础”。届时，可能还将有针对乌克兰领土的入侵行动与线上攻击协同推进。英国政府也指责俄罗斯格鲁乌黑客在上周针对乌克兰军方和国有银行网站的在线服务发动了 DDoS 攻击。

2 月 21—23 日前后，第三轮攻击——HermeticWiper 数据擦除器、恶意文档鱼叉钓鱼攻击及 DDoS 攻击。

安全社区在 2 月 23 日观察到 HermeticWiper 攻击，报告称 APT 组织向乌克兰上百个机构投递了 HermeticWiper。乌克兰多个政府部门网站和银行业务遭到网络攻击。乌克兰数字转型部部长米哈伊洛·费多罗夫（Mykhaylo Fedorov）称，乌克兰遭遇新一轮大规模分布式拒绝服务攻击。同时，据安全人员观察，2021 年年末开始大量乌克兰用户遭到疑似 APT 组织的恶意文档鱼叉钓鱼攻击，攻击者利用诱饵文档释放并执行 vbs 脚本，通过创建计划任务的方式完成恶意文件的驻留，这些 vbs 文件名多数以 .log 结尾，且经过高度混淆。相关攻击活动的受影响用户规模和活跃度在今年 2 月 21 日激增并达到顶峰。

另外，在 2 月 23 日，乌克兰境内多个政府机构（包括外交部、国防部、内政部、安全局及内阁等）及两家大型银行的网站再次沦为 DDoS 攻击的受害者。专注监测国际互联网状态的民间组织 NetBlocks 还证实，乌克兰最大银行 PrivatBank、国家储蓄银行（OschadBank）的网站也在攻击中遭受重创，目前与政府网站一同陷入瘫痪状态。

（二）虚假信息影响心理认知

当地时间 2 月 24 日，俄罗斯总统普京宣布在顿巴斯地区发起“特别军事行动”。俄乌紧张局势持续升级，而网上相关信息在此之前和之后，也是铺天盖地，难辨真假。在全球关注的众多大事件发生后，都会有大量虚假信息在网上出现，但本次的虚假信息传播，显然范围更广，规模更大。在全球各个国家不同语言的平台，关于当地局势发展情况的相关虚假信息都在不断传播泛滥。

网络攻击方面俄罗斯实力强大且蓄谋已久抢得先机，那么在信息战上的交锋，俄乌双方都是不遗余力，难分胜负。战争进行中，大量战场图像信息在网络发布，但其中混入了很多虚假信息，要么嫁接错误的视频图像和音频，要么伪造官方发布，要么半真半假，利用机器人农场快速投放和传播。乌克兰居民还报告说收到了假短信，称该国的 ATM 取款机无法正常运作，网络安全专家说，这可能是一种恐吓策略。乌克兰国家安全与国防委员会信息安全和网络安全处处长纳塔利娅·特卡丘克也表示，网络攻击者窃取情报信息和个人数据，试图破坏稳定、抹黑和操纵国家。

这些是传统舆论战心理战的升级版——通过网络空间发布有利于己方和不利于对方的虚实信息，混淆视听，或试探对手反应，或震慑对方心理，或影响判断认知，以收到不战而屈人之兵，或在全球范围内收割同情和支持的目的。目前，开战以来，俄乌双方真实战况到底怎么样，估计不少人都困扰不已。

（三）更多力量卷入网络对抗

随着冲突战争推进，有更多力量正在卷入网络战中。

2 月 27 日，乌克兰数字化转型部部长米哈伊洛·费多罗夫在社交媒体上称，基辅正在组建“IT 部队”，“继续在网络战线上作战”，并公开喊话马斯克，要求他为乌克兰提供星链终端。马斯克随即回复称，星链服务系统已在乌克兰启动，而且“很活跃”，乌克兰可以通过正在运行的星链卫星使用宽带服务。马斯克同时承诺，将为乌克兰提供更多终端。

据报道，疑遭网络攻击，俄罗斯克里姆林宫（kremlin.ru）、联邦政府（government.ru）和国防部（mil.ru）在内的许多俄罗斯网站下线。

二、俄乌网络战的四个特点

本次俄乌军事冲突具备明显的伴生网络战的特点。对于发生在非交战期间的某一具体网络攻击行为是否是战争行为，在国际上目前尚没有清晰的界定，也是各方一直在探讨的问题。

但伴随新一轮俄乌军事冲突之中交战双方的多级、

多次网络攻击波，纳入战争行为基本上应无异议。

这次正在发生的网络战具有下列特点。

1. 范围更广、力度更大

俄乌冲突中的网络攻击发生时间长，波及面广，在双方都涉及到政府网站、银行等各类信息基础设施，且伴随冲突的进行，一轮一轮的网络攻击不断升级扩大。2 月 15 日的网络攻击，据称是乌克兰遭遇的有史以来最大的网络攻击。在乌克兰检测到的擦除恶意软件也影响了乌克兰在拉脱维亚和立陶宛的政府承包商，这表明网络战攻击很可能会“溢出”到其他国家。

2. 紧密伴随军事行动

对于本次俄乌冲突中的网络战，网络安全平台 Vectra AI 首席执行官希特什 · 谢斯（Hitesh Sheth）认为，是“在人类历史上第一次，网络攻击已经成为了一项重要的武器”。从时间上来看，网络攻击的高峰也与战争推进步调一致。例如，2 月 23 日的 DDoS 攻击发生即在普京下令全面入侵乌克兰前大约 12 小时。这与俄罗斯在格鲁吉亚的南奥塞梯出兵有相似之处，美国陆军上校 Bob Killebrew (retd) 在《小型战争杂志》发表的一份报告中指出，俄罗斯的网络攻击是与常规攻击同步使用的。

3. 社会公众心理战意义更大

网络攻击理论上具备攻击核心基础设施的能力，并造成破坏性打击，但在本次冲突中，这种情况到现在尚未被观察到。更大的意义似乎是对社会公众施加心理影响，从而达到心理战的目的，起到瓦解分化的作用。

4. 毁灭性行动或将伴随而来

在网络攻击中，乌克兰一再成为主要受害者，而俄罗斯自然而然被认定是幕后黑手。但是，针对西方社会的指责，俄罗斯表示，其“以前没有、现在也没有在网络空间进行过任何‘恶意’行动”。

无论是技术和证据怎样，俄罗斯的概不认账激起了乌克兰、欧美等国家的一再指责，称乌克兰遭受网络攻击是俄罗斯对乌克兰采取侵略行动的例证。2 月 24 日，负责乌克兰政府和企业网络安全的企业赛门铁克、ESET 称，乌克兰政府和金融机构大批信息系统数据遭到破坏。

乌克兰政府据此声称，此次遭受的网络攻击力度空前。乌克兰国家安全和国防委员会副秘书长谢尔希 · 德梅迪克（Serhiy Demedyuk）称，“对网站的篡改只是第一步，毁灭性行动将伴随而来，我们预感在不久的将来将有灾难发生。”

三、混合战争已是大势所趋

战争的目的是军事与政治目标，而网络攻击可以在减少杀伤力的情况下，达成战争目的。俄罗斯是世界公认的网络战力强国，从 2014 年第一次俄乌军事冲突开始，以俄罗斯为主，双方就开始大打网络战。

2008 年俄罗斯对格鲁吉亚的战争可能是第一次真正的混合战争，传统的军事力量和黑客力量结合在一起。但鉴于格鲁吉亚的互联网普及率低（当时约有 7% 的格鲁吉亚人使用互联网），以及相对简单的网络攻击，结果只是摧毁和破坏了大量政府网站，因而更像是网络战争的预演。

本次俄乌冲突再次印证，网络攻击伴随现代军事行动必将是信息时代战争形态的大势所趋。但从更广更长的视角看，网络战还存在许多需要国际社会进一步观察和认识的问题。

譬如，目前还没有国际公认的标准来判定一个国家发动的网络攻击是否等同于武装攻击，后者可能会引发军事回应。目前还没有任何具有法律约束力的国际文件，明确规范网络空间的国家间关系。如果交战国在和平时期违反国际法，或在战争时期违反武装冲突法，则国际法允许自卫和应对武装攻击。除了什么构成网络空间的武装攻击，现有国际法的哪些条款适用于网络空间的战争行为尚不明确。

当地时间 2 月 27 日，俄罗斯总统普京已经命令俄战略威慑力量进入“特殊战备状态”的消息传开，人类又一次感受到核恐怖并不遥远。

此前，全球似乎达成了广泛默契——太空系统和核指挥与控制系统是神圣不可侵犯的，迄今为止还没有报道反应，伴随军事打击发生了针对核力量指挥控制系统的网络攻击。

目前，我们没有看到一场全面的网络战争，笔者也非常担忧，人类理智究竟能否战胜狂热，不去突破网络战的边界。

俄乌网络战六大安全警示

作者 公关部 张雪丹

在俄乌冲突这场数字时代的第一次大规模战争中，网络空间对抗呈现出更大攻击范围、更多阵营参与的特点，给这场战争增加了许多不确定性。

俄乌双方，乃至其身后各方势力在网络对抗方面的行动，以及产生的系列反应，给我们带来值得深思的警示。

一、网络攻击成先发制人的武器：打响数字时代战争第一枪

在俄乌开战前的两个月，乌克兰重要政府机构和国有银行就遭受了三次大规模网络攻击，导致网站瘫痪或被迫暂时关闭。在正式交火后，乌克兰的互联网服务更是严重中断。在这一时间段中，奇安信司南大网威胁监测平台监测到多起针对乌克兰重要网站的 DDoS 攻击事件。

数据显示，伴随着乌克兰局势的恶变，1 月 8 日就出现了 DDoS 攻击事件；2 月 13 日之后攻击强度加大，并在 2 月 23 日后达到顶峰。

这一阶段，网络攻击主要集中在乌克兰的政务、金融设施上，主要受害网站包括乌克兰总统网、乌克兰国家公务员事务局、乌克兰政府新闻网站、乌克兰最大银行 Privatbank、国家储蓄银行网站等。

分布式拒绝服务攻击致使多个乌克兰政府网站下线，一些银行网站关闭，银行无法提供服务。2 月 24 日，乌克兰国家紧急事务部门称，因为遭受网络攻击威胁，乌克兰临时切断互联网。

这些“先行”的网络攻击，被乌克兰及其盟友归咎于俄罗斯。其中，1 月 15 日，乌克兰数十个政府网站遭篡改、瘫痪，部分数据遭清除，白俄罗斯网络间谍组织 UNC1151 被认为是幕后操纵者之一；2 月 15 日发生的大规模 DDoS 攻击事件中，俄罗斯情报机构 GRU 被控涉身其中。

针对乌克兰遭受 DDoS 网络攻击行为被视为战争前兆。但多年来，乌克兰持续遭受网络攻击，网络安全防护建设在被动中步履维艰，在身处战场时只能向外界求援。

2 月 17 日，乌克兰、英国和波兰三国外交部发表联合声明称，乌克兰同意与波兰和英国制定三边合作备忘录，合作侧重于网络安全、能源安全及加强战略沟通，以打击虚假信息；2 月 22 日，网络快速反应小组项目的牵头国立陶宛正式宣布了在网络防御领域帮助乌克兰的消息。

警示：现代战争早已进入混合战阶段，“军事热战”之前网络战先行，未雨绸缪方是最佳应对之道。

面对不可避免、随时可能袭来的大规模网络攻击，我们需要警惕，政府、银行等关键设施等网络安全体系能否经受住冲击？是否有足够的安全人员和能力快速应对攻击？在和平时期，需要通过贴近实战的大规模攻防演练，检验安全建设成果、进行查缺补漏，提升应对实战攻击的能力。这是俄乌冲突给国内的第一个警示。

二、网络攻击与现实战场交织：关基设施成攻击重点

自俄乌网络攻击开始以来，关键基础设施就成为攻击的重点。乌克兰政府机构、银行网站遭网络攻击瘫痪，电信基础设施经常性出现中断服务，俄罗斯政务等基础设施也频繁出现无法访问的情况。

2 月 24 日，乌克兰国家紧急事务部门称，因遭受网络攻击威胁，乌克兰已经临时切断互联网。据 NetBlocks 互联网状态监控数据，自 2 月 24 日起，乌克兰多个城市出现网络中断情况。2 月 26 日，乌骨干网运营商 GigaTrans 出现严重中断。经分析，电信网络中断是因为停电、网络攻击、蓄意破坏等导致。

2 月 24 日起，俄罗斯出现部分政务系统无法访问的情况：2 月 24—25 日，俄罗斯国家媒体 RT 电视台网站短暂出现无法访问；2 月 26 日早，克里姆林宫官网、俄罗斯外交部、红星电视台等多家俄罗斯网站处于不稳定状态，部分用户无法正常打开页面。

俄乌冲突中的网络攻击集中在政务、金融、电信等基础设施范围内，尚未波及到直接影响民众生活的水、电等关键性基础设施。但据《华盛顿邮报》15 日报道，美国政府认为，俄罗斯黑客已经渗透到乌克兰的军事、能源和其他关键的计算机网络，如果俄罗斯政府选择攻击乌克兰，他们有能力破坏这些系统。

俄罗斯国家计算机事件响应与协调中心在当地时间 24 日发布警告，提醒国内关键基础设施运营商“计算机攻击强度增加的威胁”，并表示应考虑任何没有“可靠确定”原因的关键基础设施运行故障，可能是计算机攻击的后果。

作为俄乌冲突背后的重要力量，美国“已准备好应对措施”，应对俄罗斯对美国企业和关键基础设施可能发动的网络攻击。

警示： 在网络空间和物理世界协同的混合战争中，电信、能源等关键基础设施无疑是攻击的重点，提升安全防护能力，确保战时的稳定可用是安全防护的重中之重。这是俄乌冲突给出的第二个警示。

三、攻击数量激增、手段多样、组织众多：安全防护难度空前

根据 Check Point 研究部门 (CPR) 的数据，在俄罗斯发起战争后的前三天，针对乌克兰军队和政府部门的网络攻击增加了 196%。美国网络安全公司 Imperva 数据也显示，当前全球发生的所有网络攻击活动，10 次有近 9 次发生在俄罗斯或乌克兰。

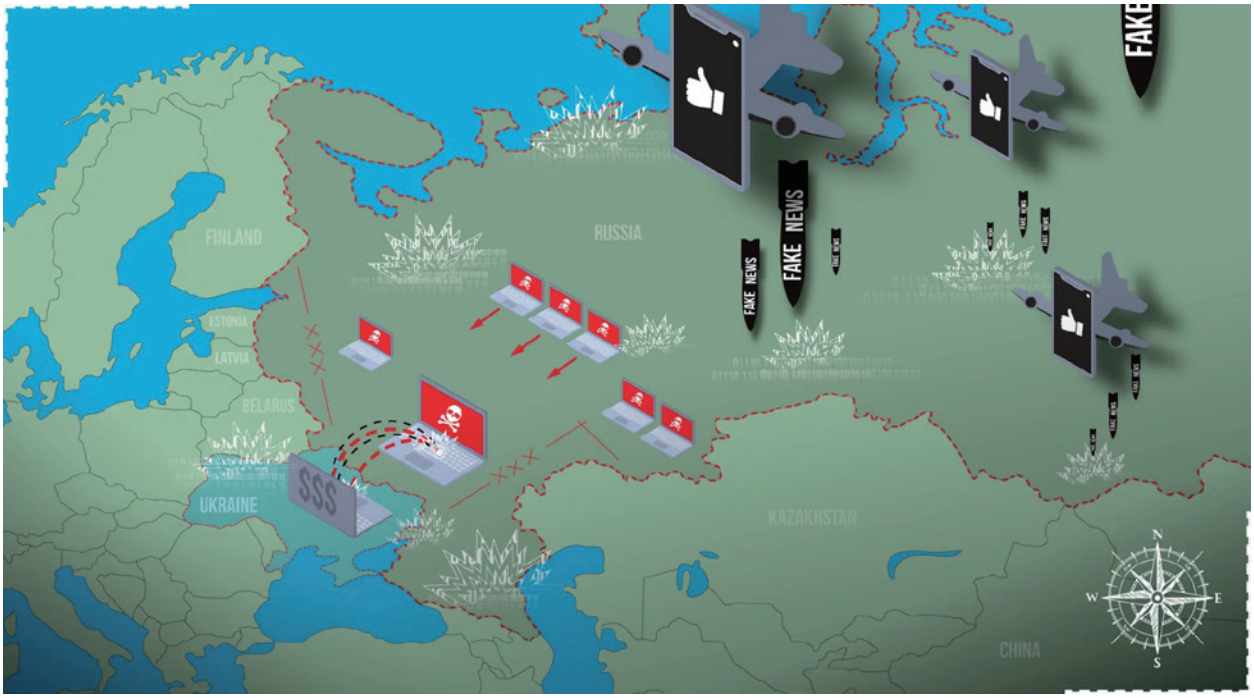
本次俄乌网络战中，双方的攻击手段多样，包括数据擦除软件、钓鱼攻击及 DDoS 攻击；安全研究人员先后发现了 WhisperGate、HermeticWiper、IsaacWiper 等恶意软件。

此外，参与攻击的队伍众多，其中不仅有俄罗斯、乌克兰两国国家背景的攻击组织，还包括乌克兰招募的包括匿名者组织及各国黑客的 IT 部队。事实上，整个网络安全社区都在选边站，无论是俄罗斯还是乌克兰。Check Point 威胁情报主管 Lotem Finkelstein 认为：“这是历史上第一次任何人都可以参与的网络战。” 乌克兰当局估计，约有 400,000 名跨国黑客自愿帮助应对俄罗斯的网络攻击。

根据推特账户 Cyberknow 统计，截至 3 月 20 日，共发现 77 个，其中 51 个支持乌克兰，25 个支持俄罗斯，1 个机构情况未知。该推特账户定期更新俄乌网络战的主要攻击组织名单。

攻击组织瘫痪网站与重要的政府、金融与电信服务，或者涂鸦反战信息、泄露黑客组织的数据与军事人员个人信息。参与网络攻击的队伍众多，大大增加了防护的难度。

在俄乌战争开始后，具有多个附属团体的匿名者黑客组织（Anonymous Group）宣布对俄罗斯发动网络战，鼓励其他黑客组织采取行动。据报道，匿名者黑客组织先后破坏了俄罗斯天然气工业股份公司的网站、国家级新闻频道 RT，并关闭了俄罗斯航天局“Roscosmos”的控制中心。3 月 7 日，匿名者黑客组织声称入侵了俄罗斯国家电视台俄罗斯 24、第一频道和莫斯科 24，并且播放了许多乌克兰战争画面。3 月 8 日，匿名者黑客组织接管了 400 多台俄罗斯摄像机，并在 backenemylines.live 网站上分享了被黑摄像头的实时信息。此外，其所属的 Network Battalion 65 声称，入侵了俄罗斯网络安全公司卡巴斯基，并扬言将泄露卡巴斯基的源代码。此外在乌克兰进行军事行动的 12 万名俄罗斯军人的个人信息可能遭泄露。



警示：现代网络战的攻击手段多样化、数量激增，以及众多潜在攻击者，提醒网络安全防护难度巨大。

四、网络攻击外溢风险：警惕攻击的连带危害

面对激烈的俄乌网络冲突，各国纷纷拉响重点部门的安全警报。这当然不会是过度反应：由于全球技术的共性，因系统漏洞遭受攻击时，全球其他国家和机构也容易遭受相同的攻击。

俄乌之间的网络攻击，不仅会对乌克兰和俄罗斯的平民造成影响，还会对全球产生溢出效应。实际上，一些网络安全公司表示，在乌克兰检测到的擦除恶意软件已经影响到拉脱维亚和立陶宛等邻国。这表明网络战攻击已经“溢出”到其他国家。

安全公司 Crowdstrike 高管亚当 · 梅耶斯认为，“尽管尚未有证据表明已有网络攻击瞄准西方实体，但针对乌克兰的扰乱性或毁灭性网络攻击，很有可能带去附带影响。在乌克兰设有分支机构、与乌克兰有业务往来或依靠乌克兰供应链的西方公司都有可能受到影响。”

网络安全公司赛门铁克研究员表示，在 2 月 23 日的攻击中，针对乌克兰的攻击使用了一种新型的擦除数据恶意软件，该恶意软件也在拉脱维亚和立陶宛活跃，这可能表明有意或无意的区域传播。

这样的担忧并非没有前兆：2017 年 NotPetya 恶意软件对乌克兰某会计软件提供商的入侵，最终却影响了全球超 65 个国家，造成经济损失超过 100 亿美元。包括航运巨头马士基、制药巨头默克、联邦快递欧洲子公司、法国建筑公司圣戈班、食品制造商亿滋国际及制造商利洁时等在内的跨国公司均受到重创。

针对俄乌网络攻击，各国纷纷采取预防措施，未雨绸缪：1 月 28 日，英国国家网络安全中心（NCSC）发布指南，敦促英国机构组织增强其网络安全弹性，以应

对乌克兰及其周边地区的恶意网络事件；2 月 9 日，欧洲中央银行要求银行业就俄罗斯潜在网络攻击做好准备；2 月 11 日 CNN 报道，美国安全和情报机构开会讨论，为潜在的俄罗斯黑客威胁做好准备。加拿大、波兰、新加坡、澳大利亚等国政府也纷纷对国内相关机构和企业发布安全预警。

安全专家忧虑俄乌双方的网络攻击可能给全球网络空间带来难以避免的连带损害。许多机构在警告，这场冲突的网络战会蔓延到乌克兰境外。特别值得当心的是可能与俄罗斯受制裁机构有关的组织，尤其是在金融服务和能源领域。也有专家警告说，俄罗斯在地面军事上的推进不力，可能导致俄罗斯进行对等报复，与西方国家之间展开“全球网络战”。

警示：网络攻击的溢出效应意味着网络攻击的负面影响很难限定在物理的国家边界内。针对俄乌之间日趋激烈的网络攻防，需时刻做好应对准备，维护自身关键信息基础设施安全，避免受到溢出效应的影响。

五、全面出口管制：核心技术依赖暴露短板

针对俄乌冲突，美国、欧盟和英国对俄罗斯实施的制裁和出口管制，限制包括技术在内的美国商品，以及使用美国设备、软件和蓝图生产的外国商品出口到俄罗斯。

欧美高科技巨头也参与对俄罗斯的制裁，宣布暂停在俄罗斯的所有业务。英特尔与 AMD 停止对俄罗斯的计算机芯片供应；亚马逊、苹果、谷歌、戴尔、惠普、Twitter 、Facebook、Netflix、诺基亚、SAP、甲骨文等企业，均已暂停在俄罗斯发货。

根据报道，以美国为首的国家对俄罗斯实施制裁措施包括对半导体、电信、加密安全、激光、传感器、导航、航空电子设备和海事技术的广泛限制。随着大量科技企业发布暂停销售和业务运营的消息，分析人士认为，持续制裁将会导致俄罗斯的 IT 服务中断。这可能有些危言耸听，但俄罗斯核心技术与产品对海外的依赖还是暴露出其产业链上的短板。

俄罗斯在推进自主可控方面已经做了诸多工作。从

2015 年开始，俄罗斯通过对国有企业和政府机构采取各种激励和惩罚措施，推动迁移到俄罗斯制造的软件和硬件。

随着俄罗斯基于 Linux 的国产操作系统——Astra Linux 的开发完成，其操作系统国产化程度进一步提高；俄罗斯政府机构和企业早已在测试基于 Baikal-M 微处理器的硬件解决方案。

但目前，俄罗斯没有能够制造先进计算机所需的高端半导体的产业，而是依赖从日本、韩国及我国台湾进口所需的高端半导体产品。

如果没有持续的高端半导体供应，俄罗斯企业、电信公司和云服务提供商将很难维护和发展未来的技术基础设施。GlobalData 分析师埃米尔 · 哈利洛维奇 (Emir Halilovic) 表示：“任何类型的数据中心运营都将难以继续进行，并且随着制裁制度的继续实施，其影响将会显现。”

据俄《消息报》3 月 1 日报道称，针对网络威胁，俄罗斯已做好启用本国互联网系统 Runet。Runet 是俄罗斯出于国家网络防御目的而构建的内部局域网。2019 年 5 月俄总统普京签署《互联网主权法》，推动俄罗斯互联网基础设施逐步摆脱对境外网络的依赖。2019 年底俄罗斯宣布成功完成断开国际互联网测试，Runet 国内网初成。

警示：在核心技术领域实现自主可控和突破，减少和摆脱对国外技术的依赖，是在战时确保系统正常运行、经济稳定的重要保障，更是应对高等级网络攻击威胁的根本手段。

面对日趋复杂的国际形势和地缘冲突，我们需要加快突破网络安全核心技术，推动我国网络安全产业高端化、自主化、体系化发展，为加快建设网络强国提供有力的安全保障。

六、“全球直播”的俄乌冲突：社交媒体平台的争夺与控制

得益于网络和社交平台的发达，这次的俄乌冲突基本是在全球“同步直播”。俄乌双方都积极利用网络和社交媒体发布战场信息，以期能够影响战局。社交媒体成为又一个重要争夺阵地。

在社交媒体上，有关俄乌冲突的图文、视频消息层出不穷，真假难辨。推特称，自乌克兰冲突开始以来，用户每天在推特上发布约 4.5 万次指向官方媒体的链接；乌克兰“IT 军队”的招募和任务发布甚至都是通过 Telegram 进行的。

随着战争的推进，社交平台成为各方争取或施压的对象。乌克兰政府最早呼吁苹果、推特、谷歌、网飞等公司停止其在俄罗斯的服务；2 月 27 日，欧盟委员会主席冯德莱恩宣布将在欧盟封禁俄罗斯官方媒体；3 月 1 日起，推特开始对所有包含俄罗斯官方媒体链接的推文贴标签，以便让用户知道信息源，苹果、Meta、网飞、微软等平台也纷纷采取了限制访问、限流降级、限制广告等措施；据英国路透社 2 日报道，欧盟针对今日俄罗斯和俄罗斯卫星通讯社的禁令，已于当天正式生效。

在此次俄乌冲突中，乌克兰在社交媒体的利用上显然更胜一筹。2 月 26 日，乌克兰国防部在推特上为俄罗斯士兵的亲属开通了名为“从乌克兰活着回来！”的热线电话。有效开展“攻心为上”舆论战。2 月 22 日起，乌克兰总统泽连斯基在推特、YouTube 等平台上接连发声，呼吁国际社会制裁俄罗斯、支援乌克兰。

与乌克兰全民利用社交媒体宣传战争惨烈和成果从而博取同情不同，俄罗斯官方媒体则在社交平台和多国被禁，失去了争取主动和赢得支持的话语权。

警示：具有国际影响力的社交平台在重大国际冲突中具有特殊角色和作用，发挥着赢得支持和同情乃至影响和重塑现代战争的作用。

这提醒我们要重视社交媒体，尤其是全球化平台在重大国际冲突中的特殊角色。一方面支持和发展具有全球影响力的我国社交媒体平台，把握关键时期的话语权；同时也要研究全球社交平台的传播特点，适应 UGC 时代的传播规律，营造更好的国际舆论环境。

俄乌网络战期间的攻击组织

（基于推特账号 Cyberknow 3 月 20 日更新）

Anonymous 派系	支持国家	攻击手法	信息公布平台
Anonymous	乌克兰	DDoS/Hack	Twitter（推特）
BlackHawks	乌克兰	DDoS/Hack	Twitter（推特）
Anon Liberland & PWN-BAR	乌克兰	DDoS/Hack	未知
LiteMods	乌克兰	Psyops	Twitter（推特）
SHDWSec	乌克兰	Hackivism	Twitter（推特）
RootUser	乌克兰	Radio	Twitter（推特）
N3UR0515	乌克兰	DDoS/Hack	Twitter（推特）
PuckArks	乌克兰	Psyops	Twitter（推特）
GrenXPaRTa_9haan	乌克兰	数据泄露	Twitter（推特）
YourAnonNews	乌克兰	Psyops	Twitter（推特）
DeepNetAnon	乌克兰	Radio/Hack	Twitter（推特）
Anonymous Younes	乌克兰	DDoS/Hack	Twitter（推特）
0xAnonLeet	乌克兰	DDoS/Hack	Twitter（推特）
AnonGhost	乌克兰	DDoS/Hack	Twitter（推特）
Anonymous Romania	乌克兰	DDoS/Hack	Twitter（推特）
Shadow_Xor	乌克兰	数据泄露	Twitter（推特）
PuckArks	乌克兰	破坏	Twitter（推特）
Vest1geSec	乌克兰	Hack/ DDoS	Twitter（推特）
Squad303	乌克兰	DDoS/ Psyops	Twitter（推特）
AlphaDisiak	乌克兰	勒索攻击	Twitter（推特）
GhostSec	乌克兰	黑客	Twitter（推特）
DDoS Secret	乌克兰	数据泄露	Twitter（推特）

国家背景组织	支持国家	攻击手法	信息公布平台
GhostWriter UNC1151	俄罗斯	Hack	未知
SandWorm	俄罗斯	Hack	未知
Gamaredon	俄罗斯	Hack	未知
DEV 0586 APT	俄罗斯	Hack	未知
DEV 0665 APT	俄罗斯	Hack	未知
FancyBear APT	俄罗斯	Hack	未知
IT Army of Ukraine	乌克兰	DDoS	Twitter（推特）
IT Army of Ukraine Pysops	乌克兰	Psyops	Twitter（推特）
Internet Forces of Ukraine	乌克兰	Psyops	未知
MuStandPanda APT	未知	Hack	未知

亲乌克兰团体	支持国家	攻击手法	信息公布平台
BlueHornet	乌克兰	Hack	Twitter（推特）
KelvinSecurity Hacking Team	乌克兰	Hack	Twitter（推特）
GNG	乌克兰	DDoS	Twitter（推特）
NB65	乌克兰	Hack	Twitter（推特）
RaidForums2	乌克兰	DDoS	Twitter（推特）
ContiLeaks	乌克兰	数据泄露	Twitter（推特）

GhostClan	乌克兰	DDoS/Hack	Telegram（电报）
1LevelCrew	乌克兰	DDoS	Twitter（推特）
Spot（ATW）	乌克兰	Hack	Twitter（推特）
Hydra UG	乌克兰	Radio	Twitter（推特）
SecJuice	乌克兰	OSINT/Psyop	Twitter（推特）
v0g3lSev	乌克兰	Hack	Twitter（推特）
Belarusian Cyber-Partsans	乌克兰	勒索	Twitter（推特）
DDos Secrets	乌克兰	数据泄露	Twitter（推特）
NB65-Finland	乌克兰	DDoS	Twitter（推特）
Monarch Turkish Hacktivists	乌克兰	Defacement	未知
Shadow_Xor	乌克兰	未知	Twitter（推特）
The connections	乌克兰	未知	Twitter（推特）
TrickLeaks(new trickbots)	乌克兰	数据泄露	Twitter（推特）
Cystal_MSF	乌克兰	Hack/DDoS	Twitter（推特）
Rabit Two	乌克兰	Hack/DDoS	Twitter（推特）
K3moryK1tten	乌克兰	Hack/Support	Twitter（推特）
SecDet	乌克兰	Hack	Twitter（推特）
BeeHive Cybersecurity	乌克兰	Phishing/Hack	Twitter（推特）
Cyber_legion_hackers	乌克兰	Defacement	Twitter（推特）
Sand For Ukraine	乌克兰	Hack/DDoS	Telegram（电报）
Ring3API	乌克兰	Hack	Twitter（推特）

亲俄罗斯团体	支持国家	攻击手法	信息公布平台
RedBanditsRU	俄罗斯	Hack	Twitter（推特）
Free Civilian	俄罗斯	数据泄露	网站
CommingProject	俄罗斯	数据泄露	网站
Stormous Ransomware	俄罗斯	勒索	Telegram（电报）
Hydra（Digital Cobra Gang）	俄罗斯	Dox/DDoS	Twitter（推特）
Xaknet	俄罗斯	Hack	网站
Killnet	俄罗斯	Hack/DDoS	Telegram（电报）
RaHDit	俄罗斯	Hack	未知
Devilix-EU	俄罗斯	未知	Twitter（推特）
Drag0n	俄罗斯	劫持	Twitter（推特）
404 Cyber Defense	俄罗斯	DDoS	Twitter（推特）
ECO	俄罗斯	DDoS/Hack	Twitter（推特）
WheretheGoons	俄罗斯	Hack	Twitter（推特）
FfboyG	俄罗斯	Psyops/DDoS	Twitter（推特）
Conti Rasomware	俄罗斯	勒索	Onion
Punisher_346	俄罗斯	Psyops	Twitter（推特）
Lorec53	俄罗斯	Hack	未知
DdoS Hacktivist Team	俄罗斯	DDoS	Telegram（电报）
Cyberwar_world	俄罗斯	Hack/DDoS	Telegram（电报）

俄乌网络战时间线

俄乌战争，网络战打响第一枪。自俄乌战争爆发以来，乌克兰和俄罗斯之间的网络攻击数量“惊人”。乌克兰当局估计，约有 400,000 名全球黑客自愿帮助应对俄罗斯的网络攻击。随着来自各地的志愿者加入战斗，俄乌冲突相关的网络战正在激增。下面是截至近期的主要攻击活动与各方应对。

1.14–1.15

· 1 月 14—15 日，乌克兰 70 多个政府网站遭篡改、瘫痪，部分数据遭清除。涉及攻击手段包括 OctoberCMS nday 漏洞、数据擦除软件 WhisperGate 等。乌克兰国家安全与国防委员会副秘书长 Serhiy Demedyuk 将部分攻击归咎于白俄罗斯威胁组织 UNC1151。

2.15

· 2 月 15 日，乌克兰政府和银行遭受到大规模 DDoS 网络攻击，导致国防部、外交部、文化部及国内最大两家银行 PrivatBank 和 OschadBank 等机构的网站停止运行，两家银行的 APP 和在线支付都无法使用，部分用户收到虚假消息。美英政府将此次攻击归因至俄罗斯 GRU。

2.23

· 2 月 23 日，乌克兰多个政府、金融机构（包括外交部、国防部、内政部、安全局、内阁及两家大型银行等）再次遭到 DDoS 攻击瘫痪，数百台机器还遭到数据擦除攻击。涉及攻击手段包括 Mirai 等僵尸网络、数据擦除软件 HermeticWiper 等。

2.24

· 2 月 24 日，黑客组织“匿名者”（Anonymous）宣布对俄罗斯发起“网络战”。匿名者及相关黑客宣称，利用 DDoS 攻击瘫痪了多个俄罗斯政府和媒体网站，并获得了俄罗斯国防部的敏感数据。

2.24

· 2 月 24 日，俄罗斯总统普京宣布在乌克兰东部开展军事行动。

2.24

· 2 月 24 日，俄罗斯国家计算机事件响应与协调中心发布警告称，针对俄罗斯信息资源（包括关基）的攻击强度可能会增加。攻击旨在破坏重要信息资源和服务。

2.24

· 2 月 24 日，据路透社报道，乌克兰国家紧急事务部门称，因为遭受网络攻击威胁，乌克兰已经临时切断互联网。

2.24

· 2 月 24 日，据 NetBlocks 互联网状态监控数据，自 2 月 24 日起，乌克兰多个城市出现网络中断情况。2 月 26 日，乌骨干网运营商 GigaTrans 出现严重中断。经分析，电信网络中断是因为停电、网络攻击、蓄意破坏等导致。

2.24

· 2 月 24 日，美国商务部宣布针对俄罗斯实施全面的出口管制措施，限制包括技术在内的美国商品及使用美国设备、软件和蓝图生产的外国商品出口到俄罗斯。这是迄今为止针对一个国家实施的最全面的出口管制措施。信息安全设备、产品等也在管制范围。

2.25

· 2 月 25 日，勒索软件组织 Conti 宣布支持俄罗斯，并威胁要攻击反对俄罗斯的国家的关键基础设施。

2.25

· 2 月 25 日，匿名者组织对石油巨头——俄罗斯天然气工业股份公司发起 DDoS 攻击，破坏了俄罗斯天然气工业股份公司的网站、国家级新闻频道 RT，并关闭了俄罗斯航天局“Roscosmos”的控制中心。

2.26

· 2 月 26 日，乌克兰副总理费多罗夫呼吁全球黑客加入乌克兰“IT 军队”，来对抗俄罗斯的数字入侵。

2.27

· 2 月 27 日，乌克兰“IT 军队”，对俄罗斯和白俄罗斯的 2 个金融机构、9 个媒体和 5 个政府机关网站发起 DDoS 攻击，造成了白俄罗斯共和国国家安全委员会等 16 家官方网站停止服务的结果。

2.27

· 2 月 27 日，应乌克兰副总理的推特请求，美国公司 Starlink 创始人马斯克宣布，为乌克兰开通卫星互联网服务。

2.28

· 2 月 28 日，乌克兰“IT 军队”，对俄罗斯 2 个金融机构莫斯科交易所及俄罗斯储蓄银行和俄罗斯联邦安全局网站发起 DDoS 攻击，造成服务停止。

2.28

· 2 月 28 日，匿名者组织对白俄罗斯共和国国防部军事信息门户、白俄罗斯共和国国防部军事信息门户和 7 个俄罗斯重要政府机构发起 DDoS 攻击，还入侵了俄罗斯核能研究所并窃取了大量数据。

2.28

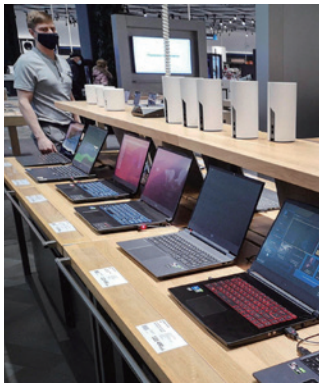
· 2 月 28 日，黑客组织白俄罗斯网络游击队声称，对白俄罗斯铁路发起攻击，成功进入控制白俄罗斯火车系统的计算机。该行动旨在为俄罗斯军队的调动制造麻烦，“减缓”驻扎俄罗斯军队进入乌克兰的速度。

3.1

· 3 月 1 日，匿名者组织对白俄罗斯 PriorBank 银行官方网站、白俄罗斯银行储蓄银行官方网站发起 DDoS 攻击。

3.2

· 3 月 2 日，乌克兰敦促约 50 家科技公司对俄罗斯的军事行动采取措施，包括游戏、电子竞技和互联网基础设施领域的科技公司。亚马逊宣布向支持乌克兰的企业和政府提供物流和网络安全支持。戴尔公司、甲骨文、Sap 公司宣布暂停俄罗斯业务。



3.3

· 3 月 3 日，乌克兰“IT 军队”——黑客志愿者发布了一系列新攻击目标，其中包括俄罗斯本土的卫星导航系统 GLONASS。

3.4

· 3 月 4 日，微软公司暂停在俄的销售，持续专注向乌克兰提供网络安全保护。埃森哲暂停在俄罗斯市场业务。备份软件公司 Veeam 停止在俄软件销售。

3.5

· 3 月 5 日，英特尔公司宣布暂停在俄罗斯的 PC 和服务器处理器销售。

3.7

·3月7日，匿名者组织声称入侵了俄罗斯国家电视台俄罗斯24、第一频道和莫斯科24，并播放许多乌克兰战争画面。

3.8

·3月8日安全应急响应基金：因应乌克兰遭受的网络攻击，欧盟27国电线部长计划设立网络安全应急响应基金，应对大规模的网络攻击。

3.11

·3月11日，宽带网络攻击：西方情报机构——即NSA和ANSSI及乌克兰情报机构——正在调查身份不明的黑客发起的网络攻击，这场与俄罗斯军事行动同时进行的攻击，破坏了乌克兰的宽带卫星互联网接入。

3.12

·3月12日，匿名者组织声称，攻击了俄罗斯国家核能公司Rosatom，窃取了该公司的数据并泄露千兆字节的数据。同日，还声称干扰了俄罗斯军事通信，捕获并共享了俄罗斯军方未加密的高频和莫尔斯电码通信。

3.13

·3月13日，俄罗斯能源子公司遭网络攻击：俄罗斯能源公司Rosneft德国子公司遭受网络攻击。Rosneft公司的IT系统受到影响，但业务或供应情况没有受到影响。

3.8

·3月8日，互联网服务提供商Lumen Technologies和Cogent Communications宣布终止俄罗斯服务。

3.11

·3月11日，俄网络安全公司网站遭网络攻击。俄罗斯信息安全公司Rostelecom-Solar表示，截至8日，2022年3月针对其网站的攻击猛增，拒绝服务（DDoS）攻击的数量已经超过了2022年2月。

3.8

·3月8日，Mandiant成立乌克兰危机资源中心，帮助机构发现应对俄罗斯入侵乌克兰相关网络威胁的办法。

漏洞情报：为什么、要什么和怎么做

作者 汪列军

为什么需要漏洞情报

漏洞从来都是网络攻防的焦点所在，因为漏洞直接或间接影响安全性的核心方面：权限，攻击者挖掘和利用漏洞获取非授权的权限，防御方定位和消除漏洞，监测和阻断漏洞的利用，使攻击者无法利用漏洞达到其目的。漏洞信息本质上是一类威胁情报，可以被用来结合组织自身的资产驱动持续的检测与响应，避免漏洞导致实际的风险。

近年来，陆续有一些厂商开始做漏洞情报，声称基于漏洞优先级排序技术（VPT，Vulnerability Priority Technology）提供更有价值的漏洞信息服务。为什么会有 VPT 这么个提法？一个大的漏洞库不能满足用户的需求吗？是的，不满足，而且是非常的不满足。要理解这个问题，我们需要对漏洞的现状有一个基于统计数据的详细分析，而这个事情其实很多所谓的专业安全厂商都没有认真做过。

一些基本的统计数据

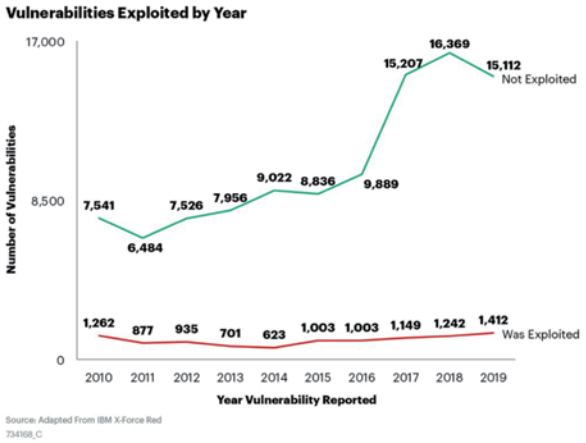
奇安信 CERT 收集了 2020 年全年加上 2021 年上半年的漏洞信息，以下是一些基本的统计。

- 漏洞总数：37478
- 0day 漏洞数：106，0.28%；其中 40+ 国产软件
- ZDI 漏洞数：450，1.2%；其中 200+ 目前无 CVE
- 无 CVE 漏洞数：10887，29%
- CNVD 漏洞数：17593，47%
- 有公开 Exploit/POC 的漏洞数：1973，5%；Exploit-DB 来源 414；PacketStorm 来源 633；Github 来源 1338；MetaSploit 来源 24
- 有野外利用的漏洞数：667，1.8%；其中 319 有公开 Exploit，348 无公开 Exploit
- APT 相关的漏洞数：30，0.08%

基于数据的分析结论

- 真正造成实际风险的漏洞只占少数

尽管存在 Exploit/PoC 的漏洞占比超过 5%，但只有1.8% 比例的漏洞有公开来源信息显示存在野外利用，所以，实际导致安全风险的漏洞在已知漏洞集中只占很小一部分。IBM X-Force 对近 10 年来的漏洞被利用情况也做过一个统计，见下图：



可以看到，这里的数据虽然跟我们的统计结果有些差异，但数量级是一样的千级。近年来，尽管每年的漏洞数量都在创新高，但被利用的漏洞数却保持得相当稳定，10% 不到。

- 关注漏洞的实际野外利用状态非常重要

有 Exploit 漏洞数量 1973，有在野利用的漏洞数 667，只有其中 319 个有公开 Exploit，大量的在野利用漏洞并没有公开的 Exploit，处于私有状态，占比 15%，所以光通过标记漏洞是否存在公开 Exploit 来判

定漏洞的现实威胁还是不够的。但是调研了一圈国内做所谓漏洞情报的，基本上看不到把是否漏洞存在野外攻击这个属性做了标记并进行持续跟踪，这也是挺搞笑的事。

· CVE 远没有覆盖绝大多数已知漏洞

无 CVE 的漏洞占比接近三分之一，因此，有大量的漏洞在 CVE 的视野之外，完全依靠 NVD 的数据是不可行的。这类非 CVE 漏洞国产软件来源占了很大比例，已知的 0day 漏洞中国产软件相关的也占了差不多一半，因此非常有必要维护一个 CVE 超集类型的漏洞库。

用户的漏洞处理痛点

通过以上的数据分析，结合实际的用户反馈，我们整理了如下漏洞处置过程中的痛点：

· 每天数以百计的新漏洞披露，我们如何才能识别出哪些漏洞是真正有威胁的部分；

· 一般情况下攻击者会比防御方能更早地知道漏洞的存在，我们如何能尽早地得到完整准确的信息，不要落后攻击者太多；

· 不要说漏洞没有补丁的情况，就算漏洞已经有了相应的补丁发布，很多场景下用户也无法随心所欲地安装补丁，是不是有快速可靠的临时解决方案来规避漏洞导致的风险；

· 在处置资源有限的情况下优先处理哪些漏洞，以最大程度减小漏洞风险的敞口；

· 如何把漏洞情报无缝地集成到组织自身的日常漏洞处理流程和机制里。

好的漏洞情报需要能回应上面这些痛点，解决或缓解用户的焦虑。

应该怎么做漏洞情报

基于漏洞情报运营实践，奇安信 CERT 认为漏洞情报的运营需要起到收集器、过滤器和富化器的作用。

具体而言，通过对一手数据源的挖掘和信息实时采集，结合威胁情报对漏洞进行多维度的属性标定，保证漏洞信息的全面性和及时性；分析团队依据完善的流程和专业经验对漏洞的影响面和技术细节进行研判，把真正重要的漏洞过滤出来，保证信息的准确性和处理优先级的可靠性；对于确认的重要漏洞，我们需要富化漏洞信息的上下文，跟踪漏洞的现时威胁状态，关联相应的安全事件，给出切实可行的处理方法，提供除补丁链接外的其他威胁缓解措施建议。

全面的多维漏洞信息整合及属性标定

漏洞情报相对传统漏洞库区别最大的地方在于对漏洞本身技术层面以外维度的持续动态跟踪，一般的漏洞库的核心信息只会涉及软 / 硬件影响面（厂商、应用及版本）和漏洞本身技术层面的评估（威胁类型、利用场景、危害大小等），这些信息还远远不够，是为了有效管控漏洞导致的风险，通常需要知道得更多：

· 漏洞是否在默认配置下存在，配置情况对漏洞可利用性影响极大，非默认配置下的漏洞其实际威胁往往远不如技术层面的定性看起来那么大；

· 漏洞相关的应用系统部署量有多大，这直接影响漏洞整体的威胁评估；

· 漏洞是否已经有了公开的技术细节、 Exploit 工具、概念验证代码（PoC），这会直接影响漏洞转变为现实的攻击；

· 漏洞是否已经有野外的利用，这体现了漏洞是否已经从潜在威胁转化为现实威胁；

· 漏洞是否已经被已知的漏洞利用攻击包或大型的僵尸网络集成作为获取对系统控制的途径，这标志着漏洞现实威胁的提升；

· 漏洞是否为 0day 或 APT 活动相关，意味着漏洞可能被用于攻击高价值的目标。

所有上面这些属性都应该通过运营被标记出来，以方便用户实现有效地处理优先级排序。

下图是奇安信 CERT 对 2021 年底核弹级漏洞 Apache Log4j 任意代码执行漏洞 (CVE-2021-44228) 的标签实例，随着新近利用此漏洞的攻击事件的发现，这些标签会随时新增和更新。

奇安信 CERT 的漏洞情报还会支持基于标签的搜索，让用户非常方便地获取匹配特定属性的漏洞集合。这些标签将来还会有对应的分类和描述，让用户能更深入地了解漏洞导致的威胁。

当然，上面所有的一切都是建立在全面收集漏洞信息的基础上，奇安信监测了多个主流漏洞数据库及数百安全厂商，跟踪了 2000+ 推特账号和 80+ 安全相关新闻源，开源信息采集结合商业数据采购，并通过各种手段挖掘新的数据源。

准确的漏洞所导致实际安全风险判定

据统计，每年增加几万个漏洞，平均到每天百级的漏洞被公开出来，如果全部对其分析验证需要巨量的资源投入，这对任何厂商和组织都是不可能完成的任务，操作层面上既无可能也无必要。事实上，每年新公开的漏洞只有极少数会被认真研究。处理流程上，奇安信 CERT 会根据漏洞的影响面和验证条件，筛选出值得深入分析的漏洞，在利用多种渠道收集或自研 PoC 进行技术验证，这是漏洞情报运营过程中专业度要求最高的环节。

2021 年，Microsoft Windows Active Directory 域服务特权提升漏洞（CVE-2021-42287)14、Apache APISIX Dashboard 未授权访问漏洞（CVE-2021-45232）、Grafana 未授权任意文件读取漏洞（CVE-2021-43798）等漏洞经过奇安信 CERT 复现并被打上“奇安信 CERT 验证”的标签，标记我们对于此类严重漏洞的存在性和可利用性的专业验证。

漏洞运营的目标也不仅仅告诉用户哪些漏洞重要，同样重要的，需要告诉用户哪些看起来高危的漏洞所对应风险名不副实。一个典型的例子是 2021 年 12 月 Log4j 漏洞爆发以后，聚光灯效应下，一些衍生漏洞随之出现，团队对那些漏洞研究分析之后确认其中绝大部分并没有实际场景下的威胁，随即发布了相关的风险通告，做了技术上的澄清。

图：奇安信 CERT 发布的澄清报告

可靠的综合性漏洞处理的优先级排序

在筛选出的重要漏洞中，大量的漏洞具有相同的

CVSS 评分，仅基于这些评分基本上很难对漏洞的实际风险做出有效的评估，其他诸如漏洞是否默认配置受影响、利用的易用性稳定性、攻击者所能接触到的存在漏洞的资产量级和漏洞利用的其他前置条件，都对漏洞的实际风险有极大影响，而这些维度的评价在 CVSS 评分体系中非常难以准确量化。

于是产生了一个疑问，目前普遍基于 CVSS 评分的高低来评估漏洞的危险程度，这样真的能准确地反映漏洞的实际风险吗?

以两个 CVSS 评分接近漏洞的对比为例：Log4j 远程代码执行漏洞（CVE-2021-44228）（CVSS 10）vs Samba 远程代码执行漏洞（CVE-2021-44142）（CVSS 9.8）。

	Log4j 远程代码执行漏洞	Samba 远程代码执行漏洞
CVSS 分数	10	9.8
是否默认配置	是	否
漏洞类型	设计问题	缓冲区溢出
利用稳定性	极其稳定	不太稳定
是否需要特定配置	否	是
网络暴露面	极大	中

通过以上对比可以看到，虽然两个漏洞的 CVSS 评分看起来相差无几，但由于一系列非 CVSS 考察维度属性的差别，导致漏洞的实际威胁天差地别，Log4j 的是真正的核弹级，而 Samba 的这个基本可以归到鸡肋级。

2021 年 CVSS 评分高于 9.0 的漏洞数量有 13000 多个，其中有 3300（ 25%）多个漏洞存在对应的 Exploit，这个比例不算低，但只有 580 多个漏洞被标记存在野外利用，占比这类高危漏洞不到 5% 的比例。所以，即便是技术层面风险度非常高的漏洞，真正被用于网络攻击的概率也不高。这个难题需要通过结合威胁情报来缓解，奇安信 CERT 的漏洞情报多维度标签为用户提供了基于漏洞现时状态进行优先级排序的可能。

NOX 安全监测平台现已收录关键漏洞 27042 个，并将漏洞按照更新时间先后进行排序，例如：Apache Log4j 任意代码执行漏洞 (CVE-2021-44228)、Google Chrome 远程代码执行漏洞 (CVE-2021-37973)、致远 OA 代码执行漏洞 (CNVD-2021-51370) 等漏洞已经被标注为“发现在野利用”并且漏洞威胁等级为“高危”或“极危”，此类漏洞建议用户参考漏洞修补方法尽快进行修补。美国网络安全与基础设施安全局（CISA，Cybersecurity & Infrastructure Security Agency）发布了一个包含 500 多个已知存在野外利用的漏洞列表，奇安信 CERT 目前已经标记了超过 4000 个在野利用漏洞，这个列表也已经对外发布，这是个每个组织都要必修的漏洞列表。

及时的与组织自身相关漏洞风险通知

目前从漏洞信息公开到野外实际利用的间隔期越来越短，大多数时候防御方是在跟攻击者抢时间，哪方先知道漏洞的存在及相应的细节，决定了谁在对抗中获胜。为了及时输出漏洞风险通知，漏洞情报的运营理想条件下需要采用 7*24 的监测处理机制，直接的厂商源头信息采集，及时研判并实时推送漏洞状态更新。我们认为如下 5 类漏洞相关的状态更新需要尽快通报，因为这些更新会渐次影响漏洞的现实危害程度：

第一，新的关键漏洞公开；

第二，发现关键漏洞的技术细节；

第三，发现关键漏洞的 Exploit 或 PoC 公开；

第四，发现关键漏洞的在野利用案例；

第五，发现关键漏洞的新修补和缓解方案。

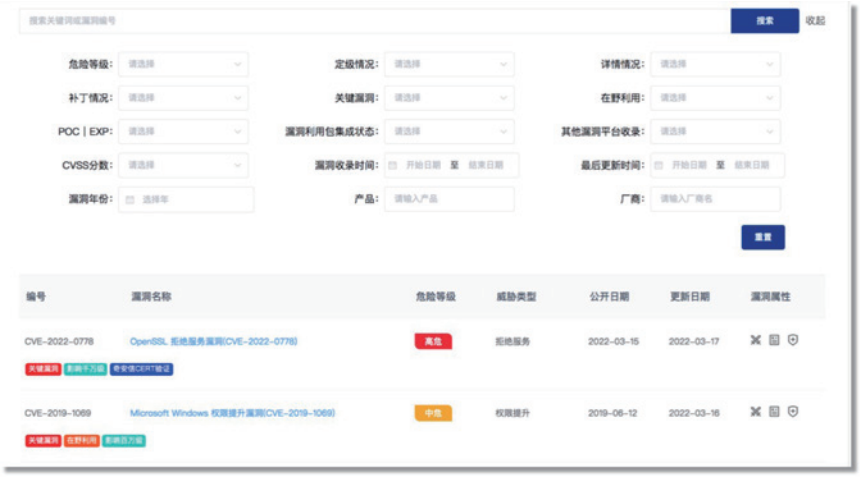
2021 年，奇安信 CERT 发布了涉及 40 多个重点厂商、300 余条漏洞的 147 篇实时安全风险通告。其中 CVE-2021-21224 Google Chrome 远程代码执行漏洞（发现时漏洞为 0day 状态）、WebLogic T3 反序列化 0day 漏洞、CVE-2021-28474 Microsoft SharePoint 远程代码执行漏洞等漏洞的风险通告，均为奇安信 CERT 使用自研 PoC 首次验证并第一时间发布。

同样重要的，为了能让组织全面地获取自身网络环境相关的漏洞信息，我们引入了全面的 CPE 信息集成，

非 CVE 漏洞（主要为国产软件漏洞）的扩展 CPE 支持，使用归一化的厂商及产品列表，包含 1000+ 软件厂商、10000+ 产品，结合主动的资产测绘精准评估漏洞影响面，第一时间提供高危漏洞定向风险通告。

对外的输出形式，不仅提供基于多维属性筛选的 Web 访问界面，还提供在线数据获取的 API 接口及离线数据包，用户可以根据自己需要集成到自有漏洞处理流程。

例如：对于 ProxyLogon 漏洞，NOX 安全监测平台持续更新 6 次安全风险通告，不断对缓解措施进行完善，最终提供了两千余字详细描述的可行操作步骤；对于 Log4Shell 漏洞， NOX 安全监测平台给出的完整处置建议涵盖了漏洞排查、攻击排查、修复版本、产品解决方案，及多种不同场景下经过验证的有效缓解措施，该完整的处置建议在奇安信多家客户单位的一线应急响应中起到了重要作用。



可行的包含详细操作步骤的处置措施

除了全面性、及时性、有效性，提供有效的缓解措施和可落地解决方案也是漏洞情报实现其价值的重要一环。很多时候，安装补丁并不是漏洞威胁处置的第一选择，因为打补丁受各种现实条件的限制。比如，在重大活动中核心服务器出于性能和稳定性的考虑，一旦安装补丁导致宕机后果不堪设想，有些补丁打完以后需要重启机器的操作是不允许的，更不用提 0day 漏洞暂时无补丁可打的情况。

因此对于很多重要漏洞，奇安信 CERT 团队还会组织相关部门开发主机或网络虚拟补丁，寻找通过调整机器配置暂时规避漏洞利用的临时解决方案，输出经过验证的 step-by-step 的操作步骤，帮助客户迅速上手进行规避风险，以后在合适的时机进行彻底修复。

不同类型用户对漏洞情报的选择要点

当前的网络安全正处在一个转型升级的上升期，网络安全体系架构已经由基础架构安全、被动防御向主动防御、反制进攻阶段进化。传统的安全思维模式和安全技术已经无法有效满足政企客户对安全防护的需要，新的安全理念、新的安全技术不断涌现。要实现有效的积极防御，很关键的一点是要具备安全情报的收集与使用能力。

对于个人用户、企业用户及安全监管单位而言，如何挑选到满足自身业务需求的优质漏洞情报，可以简单概括为一句话：“C 端用户挑产品、B 端用户挑服务、监管机构挑供应商”。

个人用户只需要确保自身的隐私安全和资产安全，不需要关注漏洞本身的技术细节，因此在漏洞情报的使用上更加依赖于其部署的终端安全产品对漏洞情报的敏感程度；企业用户基于其信息系统的复杂程度，单一的安全产品无法满足其建立企业自身漏洞检测与响应能力的需求，企业需要更加精准和定制化的漏洞情报服务，来帮助管理者迅速判别漏洞对企业业务的影响，并第一时间进行有效的漏洞处置；安全监管单位关注全网的网络安全态势，需要庞大的漏洞情报数据库支撑，更加考验漏洞情报供应商在模式化的安全产品和情报服务之上，所拥有的灵活、可变通的业务适应能力。安

规划快一步

奇安信 | BEIJING 2022

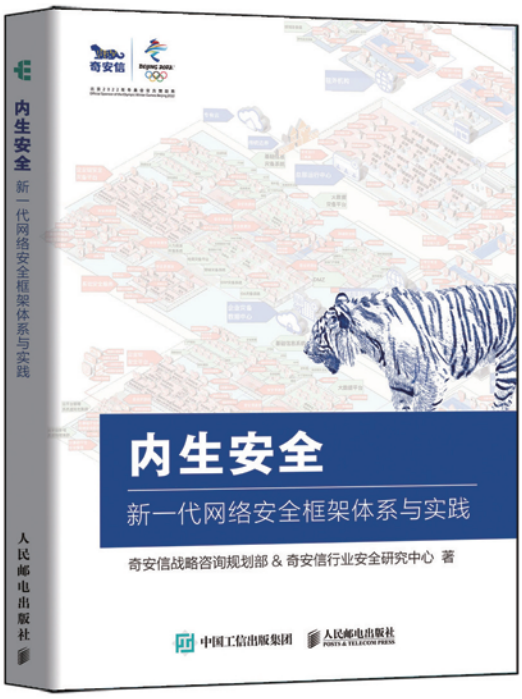
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

守护百年协和金字招牌
天眼打造“智慧医疗”安全标杆

作者 公关部 张少波

每天都有来自全国各地、数以万计的疑难重症患者到协和医院求医问诊，为了确保他们能得到及时治疗，医院的各个业务平台一刻也不能停，网络安全的保障工作可谓责任重大。

“患者性命相托的最后一站”，这句朴素的表达，道出了北京协和医院在老百姓心中的分量。北京协和医院副院长去年 12 月在国家卫健委的新闻发布会上曾分享了一组数据，“‘十三五’期间，协和医院平均日门诊量达到 1.3 万人次，其中外地患者达到了六成。”

据介绍，协和医院在解决“一号难求”的措施方面，是提升效率是其中一方面，包括采取智能药柜、一站式缴费，大大缩短了缴费取药时间；还有就是积极推进互联网诊疗，充分利用专家的碎片时间，跨越时间、空间限制，给予更多的病人服务。所有这些措施，都离不开强大的信息化基础，以及可信赖的网络安全保障。

业务与信息化密不可分 网络安全已成为“底板工程”

“一部协和史，就是半部中国医学史。” 协和作为

中国现代医学的重要发源地，自创建之初就站在了时代的前沿。建院 100 年来，协和医院始终屹立在中国医疗界的金字塔尖。在国家卫健委连续两年发布的三级公立医院绩效考核中，北京协和医院稳居全国第一。而在复旦大学医院管理研究所发布“中国医院排行榜”中，北京协和医院更是连续 11 年蝉联综合榜榜首。

医学进步离不开前沿科技的使用。据悉，北京协和医院是将计算机应用于医疗的鼻祖级机构。早在 1934 年，协和医院就购买了 IBM 公司生产的第一代商用处理机。这台穿孔卡制表机被用于协和病案的整理。

据了解，协和医院的信息化已经有 40 年的历史。1981 年，北京协和医院计算机室的成立，标志着信息化在协和医院正式启程。在 1981—2006 年间，医院在系统开发、网络建设、HIS 应用、移动医疗等方面做出了诸多有益探索，规模和深度位居当时国内领先水平。

2010 年，医院投入 6000 万元人民币，按照国家 B 级标准，规划、设计和建设了全国总面积最大的、1900 平方米的数据中心；2012 年，一体化的新 HIS 系统上线；2014 年全新院级 PACS 系统上线；2015 年通过互联互通标准化测评；2016 年 1 月，官方 App 正式推出无就诊卡预约挂号服务，无卡患者可通过手机 App 预约挂号，等就诊时再办卡。2020 年 9 月，医院在线上推出了药品配送、线上线下诊疗互转、检查一站式预约等功能，打通了患者求医问药的“最后一公里”距离。

从患者 App，到信息化基础设施建设，再到以需求为导向的全方位智慧医疗信息系统，在医院信息高速路的支撑下，协和医院的就医流程越来越短，越来越智能，患者体验度和医院服务效率也水涨船高。用协和医院的话说，“我们要用信息化做减法，要把医院和患者之间的层层流程和环节减掉”。

“信息系统安全是信息化建设的基石。没有信息系统安全，再先进的医院信息系统也会功亏一篑。” 协和医院信息中心相关负责人反复强调网络安全的重要意义。尤其随着数字化的深入，医院业务平台和网络安全已经紧密捆绑在了一起，从某种意义上来说，网络安全就等同于业务安全，成为不可或缺的“底板工程”。

四大威胁 保障关键业务不间断

近年来，针对医院的网络攻击、数据窃密等事件频繁发生，有些攻击甚至造成生命事件。协和医院结合多年和各类网络攻击斗智斗勇的经验，将医院面临的主要网络威胁，归纳了四类：

其一是肆虐的勒索病毒。

日益猖獗的勒索攻击，已经成了扑不灭的“流行病”，而信息化程度较深的医院，往往容易成为重灾区。2017 年爆发的“WannaCry”（永恒之蓝），曾让国内无数医院中招，造成系统瘫痪和数据丢失等。2019 年 1 月，国内几家医院陆续感染 GlobeImposter 勒索病毒升级变种，影响颇深。根据 Check Point Research（CPR）最新报告显示，医疗行业成为勒索软件攻击的头号重灾区，每个组织平均每周遭受 109 次攻击。

其次是数据泄露给医院临床科研、患者隐私带来的巨大风险。

很多行业的数据，需要海量才能产生价值。但对于医院来说，每条电子病历、影像数据、临床科研等，都是非常珍贵的资料，也是不法分子觊觎的目标。

国家卫健委医院管理研究所副所长王凯曾表示，医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏和泄露，势必对医疗机构的声誉、医患双方的隐私及健康安全构成严重威胁，甚至影响社会的和谐稳定。

第三是挖矿木马，蠕虫病毒等带来的威胁。

去年至今，以比特币为代表的数字加密币的价格暴涨，其中比特币单枚价格从数千美元激增至数万美元。巨大的利益驱使，使得挖矿木马泛滥，宝贵的医疗业务资源被黑客滥用于挖矿，破坏医院内部 IT 环境、数据中心的正常运行秩序，以及关键应用的交付。

最后是层出不穷的各种网络入侵。

目前，协和医院有大量的业务需要向互联网开放，如线上咨询、远程问诊、微信挂号等。对于信息中心而

言，一方面要保障医院核心业务的稳定运行，让医院争分夺秒救死扶伤; 另一方面要应对层出不穷的网络威胁，可靠的网络安全防护体系变得必不可少。

解决传统 IDS 弊端 天眼精准发现攻击、化风险于无形

北京协和医院在 5 年前部署了入侵检测设备（IDS），但是 IDS 由于时间较久，版本老旧，不支持版本升级和更新，无法应对瞬息万变的网络安全攻击形式。

同时，IDS 的威胁检测能力较弱，具有较高的误报率。“真正的攻击发现不了，大量的误报却让安全人员疲于奔命”，可以说，IDS 基本成了摆设，“不好用”“漏报、误报率太高”成为安全人员最多的吐槽。

据介绍，早在 2018 年 10 月，奇安信就组建了 5 人的安全团队，为北京协和医院提供驻场服务，并同院方技术团队一起组成网络安全组，在安全管理、风险分析、安全保障等三方面发力，全面提高医院网络信息安全处置能力。

整个 2019 年，奇安信为医院承担了协和百年 1000 天倒计时、春节、两会、一带一路、护网等一系列重保任务，帮助医院初步形成了具备攻防实战能力的“动态”安全防护体系。

2020 年 3 月，为了助力协和医院抗击新冠疫情，奇安信第一时间向北京协和医学基金会捐赠价值 230 万元的终端安全、威胁情报分析等产品及服务，增强医院的大数据研判和威胁情报分析能力。4 月，协和医院部署了天眼系统（新一代安全感知系统），旨在改变过去被动防御的状态，实现提前发现、主动防御，化风险于无形，其效果也是立竿见影。

首先是显著提升发现能力，解决了误报、漏报的矛盾。

据协和医院驻场的安服工程师介绍，天眼系统综合了威胁情报、文件虚拟执行、智能规则引擎、机器学习等技术，可以检测和发现高级网络攻击和新型网络攻击，包括 APT 攻击、勒索软件、WEB 攻击、远控木马、邮件钓鱼等高级攻击，同时基于可视化技术，清晰的展示网络中的威胁。

协和医院信息中心相关负责人表示，从实际运行来看，天眼产品对勒索病毒、挖矿木马、蠕虫病毒和网络入侵行为的发现上提供了很大的帮助，能准确识别到感染病毒事件和网络入侵行为，提升了医院对此类安全事件的发现和处置能力。

其次是全面的分析能力，尤其是异常行为的分析检测能力。

当前针对医疗行业的新型攻击手法层出不穷，利用 0Day 漏洞攻击更是屡见不鲜。为此，天眼特别增强了行为分析功能，通过运用大数据分析和机器学习技术建立网络异常行为检测模型，显著增强了未知威胁的检测准确性，以及内部违规的发现。

值得一提的是，天眼系统还支持全包取证分析，并提供线索可视化图谱拓线分析能力（威胁狩猎），能为协和医院呈现一次攻击的完成过程，帮助医院对网络攻击进行回溯和深度分析。该项功能在过去的实战攻防演习、重保等屡立奇功。

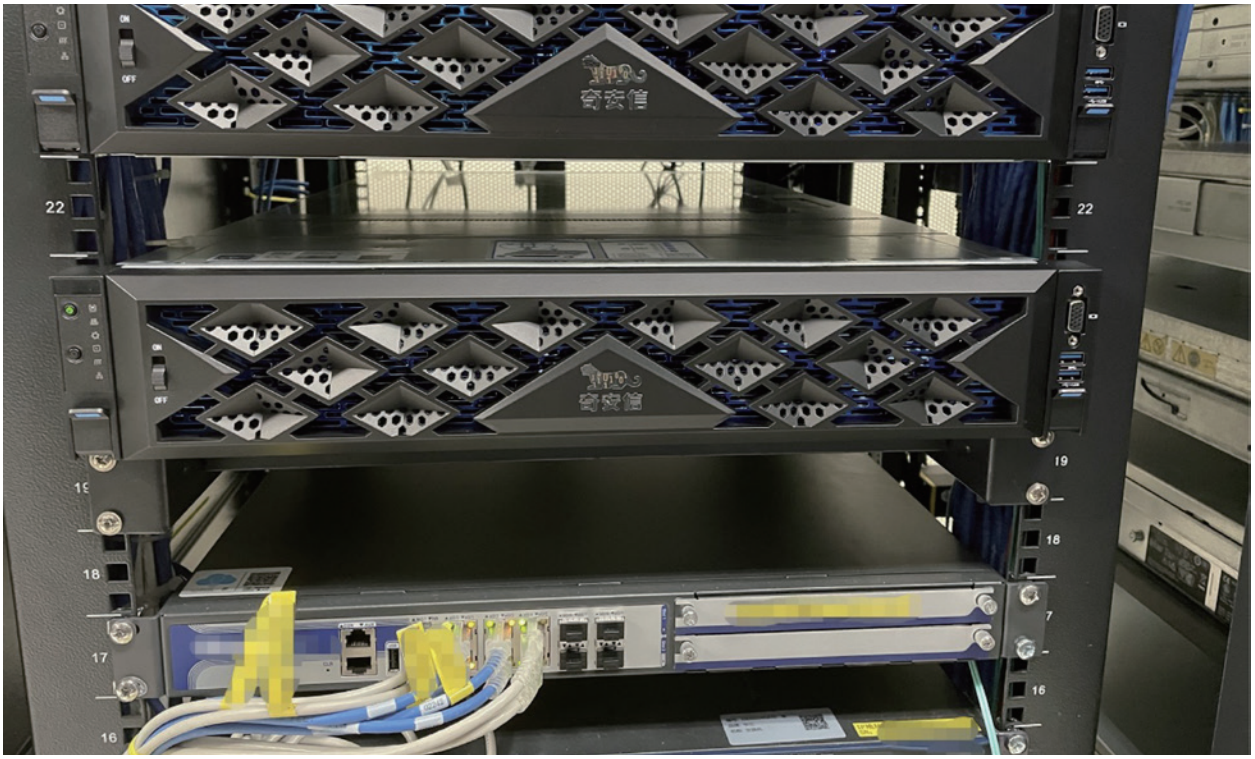
最后是旁路部署，极端条件下，不会影响业务的可用性。

“北京协和医院每天接诊量非常大，业务系统复杂而繁重，天眼采用了旁路部署的模式，对于医院来说，即便是极端和意外的情况，医院业务运行都不会产生影响。”

得益于奇安信安服团队的专业能力，以及天眼、天擎等强大的产品矩阵平台，协和医院信息中心在历次重大时间节点中表现优异，并被国家卫健委评选为重保优秀安全团队。

未来：四方面继续提升 打造体系化防护

目前医院防护体系在纵深防御、主动防御、数据安全



着手。安全管理方面需要进一步提升，后续规划主要从以下方面：

第一是持续完善纵深防御体系，充分发挥利用好现有安全产品的价值。协和医院信息中心相关负责人对纵深防御用了形象的描述，就是“进不来”“拿不走”“看不懂”“改不了”“走不脱”。“进不来”指边界防护，“拿不走”指导入 / 导出限制，“看不懂”指数据加密，“改不了”指数据完整性验证，“走不脱”指行为审计。这个过程离不开天眼系统和终端、边界防护、邮件检测等产品的协同联动能力。

第二是主动防御实现内外兼顾。Verizon 曾发布的一篇网络安全报告显示，在全世界范围内，医疗行业是内部威胁高于外部威胁的唯一一个行业。因此，医院未来会通过天眼系统等产品，强化东西向流量的监管，以及业务系统的横向隔离。

第三是稳步推进数据安全建设。9 月 1 日，我国首部与数据安全相关的法律《数据安全法》正式实施，协和医院将在身份安全、零信任、行为审计、数据敏感地图等方面强化对数据资产的安全防护。

最后是加强安全管理，落实“三同步”原则，实现网络安全工作的制度化。

“协和医院是最早将管理理念引入到 IT 部门的。”协和医院信息中心相关负责人回忆到，早在 2010 年，信息中心就开始由技术支持向信息管理职能转变。网络安全也是如此，包括技术、数据、人员和体制机制等，是一个复杂的系统。要让这个系统有效地运转，不仅要考虑产品和技术因素，还要综合技术、管理、运行等多方面的因素，网络安全工作的制度化成为下一步的重点。

“医学道路上无止境，网络安全也是一样，只有起点，没有终点。”建院 100 周年，信息化建设 40 年，北京协和医院在网络安全的道路上，还在持续探索、砥砺前行。安

初心如炬，永不灭

——走近奇安信冬奥保障总架构师尹智清

作者 公关部 孙丽芳

“北京冬奥、冬残奥会的网络安全保障，可能就是我一生中跑过最重要的一段路。”

2022 年 3 月 13 日晚，第 13 届冬残奥会在北京国家体育场圆满落下帷幕。北京冬奥会和冬残奥会技术运行中心（TOC）网络安全值班副经理尹智清离开值班室，走进了首钢园的夜色中。他开始是快走，后来跑了起来。近三年来的工作压力，在律动的步伐中，得以纾解。

酷爱长跑，完成了 60 余场全马，曾经几乎每天都要跑上十公里的尹智清最近几个月很少能尽情刷公里数。时间不允许，精力也不允许。这一切是从 2019 年 3 月的一天开始。

担压力，迎难而上

这天，尹智清被叫到奇安信董事长齐向东的办公室。一进屋，他就感到气氛很不一般。

“奇安信要竞标北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。”齐向东开门见山，现场委任尹智清负责奇安信的冬奥会赞助商应征技术方案的编制工作。

尹智清技术出身，2003 年开始做网络安全，擅长安全运营、安全规划、制度建设等领域；做过人民银行、公安部等大型央企部委的安全规划咨询；负责过奇安信面向“十四五”期间的网络安全规划“十大工程、五大任务”框架的设计，可谓奇安信的大项目“专业户”。

虽然“见过大场面”“做过大项目”，但尹智清很清楚，这和以往任何项目都不一样。这是奥运会历史上首次引入网络安全保障官方

善思考、爱长跑，动静皆宜的尹智清

赞助商，要求会极其严苛，且没有任何借鉴，但这对于奇安信、对于整个网安行业，都将具有历史性的意义。

任务艰巨而光荣，不需要动员，尹智清心里那把发令枪，“砰”地已经打响了。

“第一版应征方案是 5 月出来的，其实当时北京冬奥组委正式赞助商征集书还没出来，但我们不想打无准备之仗，所以就先凭想象、凭经验，自己先研究了一版方案。8 月我们又出了第二版。”

2019 年 10 月，北京奥组委的赞助商征集书正式公布。

“当时我们印象最深的就是招标方案里直接写了要求‘完全的、彻底的、端到端的责任’。这是结果导向的要求，要求你担托底责任，不管是设备原因、是人员原因，还是其他任何原因，只要网络安全出了任何问题都是你担责任。这种模式大家毫无经验，任何的商业投标都不会有这种要求。我们不会在任何地方看到，你买一款网络安全产品或者一项安全服务，合同里有一个条款，写着保证不出任何问题。”

要求近乎苛刻，但尹智清和团队没有丝毫退缩。最终的应征方案里，他们还专门补了一条：确保冬奥会、冬残奥会网络安全“零事故”。

抢工期，如履薄冰

2019 年 12 月 26 日，北京冬奥组委召开新闻发布会：奇安信正式成为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。

发布会举行的当天，尹智清就带着同事们进驻了冬奥组委。“一天都不能耽搁，马上就开始干活了。”

近几届奥运会中，网络黑客对奥运会的攻击持续增强。北京冬奥会面临的网络安全形势非常严峻。跨度百余公里的三个赛区、38 个场馆，近百个国家数千名运动员的交流沟通、场馆协作，需要依赖大量先进的技术。开放式 5G 网络、云计算、物联网、人工智能等技术，200 多项科技应用，使奥运网络系统空前复杂。尹智清和团队首先要对奥运网络系统做整体的安全规划。

“之前我们做规划都是聚焦在如何把网络安全做好，但在做冬奥网络安全规划的过程当中，我们要进行转变，网络安全是保证赛事准时举办，比赛第一优先。冬奥跟别的客户的形态很不一样，它的利益相关方非常多，各方关心的问题都不一样。比如，做计时计分服务的欧米茄 (OMEGA)，它关心的是比赛过程中，计时计分不要出任何问题。80 多年的奥运会我都是这样做的，你不能因为安全给我提格外的要求。面对这种现状，我们在设计过程中就要去做一些平衡。”

除了平衡不同的诉求，尹智清和团队还要弥合态度的差异。

“源讯公司是国际奥委会指定的信息系统集成商，负责将所有 IT 合作伙伴的 IT 系统和设备进行集成，包括网络安全。所以以前都是它说了算。而北京冬奥会跟历届都不一样，阿里巴巴和奇安信参与了进来，一个负责云，一个负责安全。最开始我们刚进来的时候，源讯还是有些以老大自居，觉得不需要我们去做安全的设计，你只要听我的就好了。而且对待网络安全这件事，大家态度很不一样。总体上，他们觉得奥运会其实是一个大 party，但是对于我们国家来说，奥运会是一个国家大事。”

于是，每个季度的国际奥委会网络安全高级咨询委员会，每个月的项目审计会，每周的跟源讯、阿里巴巴的网络安全周例会，疫情阶段因为远程办公每天随时拉起的视频会议……参加各种会议，沟通各方，对接不同需求，推进冬奥网络安全系统的设计和建设是尹智清 2020 年的核心工作。

期间，网络安全设计需要与信息系统建设、场馆建设同步抢工期，按照统一的安全框架，开展了一系列安全建设工作。

“我们的系统是边设计、边建设、边投入使用的。因为安全是保障，别的信息系统要上线，我们的安全必须得先上，要不然你怎么保障别人。别人可以测试，我们基本上是没有什么测试机会，上来即保障。到 2020 年底主体方案的设计工作基本就结束了。”

尹智清和同事们在冬奥网络监控室

干细活，如琢如磨

2021 年 2 月开始，现有的网络安全保障设施开始接受北京冬奥会国内测试赛和各个级别的网络安全攻防演习的考验。

“这期间系统的表现起起伏伏，也暴露出了一些问题。”

面对现状，尹智清和团队的思路很清晰。

“有问题不怕，这让我们有了改进的方向。问题基本都是出在一些安全策略的落实和安全设备的配置上。这个阶段，建设也做差不多了，我们开始真正的去干细活：所有的网络安全每条的策略配置是否合理、每项安全标准规范的定义是否能够落实、每个安全运行流程和操作步骤是否可以标准化执行到位。其实在 2019 年我们就想做标准化运行，但在那个阶段的时候，条件不具备，人不够、精力不够。目前这个阶段是一个比较好的时机。”

时机好不代表没有难度。

“难主要难在观念上。包括我们公司，其实大家对于这种常态化的网络安全运行，理解并不一样。我们的运行很多还是基于以前驻场帮着用户去做安全的那种模式。这显然无法适应奥运会的要求。因为奥运会是安全需求是结果导向的，但是我们以前干的活都不是。那时我们是服务商，客户让我们干什么，我们就干什么。而为了确保冬奥‘零事故’，不是让我们干什么我们就干什么，而是我们希望干什么，我们要推着相关方去干什么。比如，我们要协助奥委会去尽快定义并发布一些策略规范，要求各个开发商严格按照我们的信息系统的全生命周期管理去执行，尤其是要推动我们自己内部把常态化的运行做出来。很多功能规划时很美好，到实际落地时，才发现又是完全另一回事，关键还在运行。”

尹智清的想法得到了公司的全力支持。2021 年 8 月，奇安信把安服几乎全国的精英调来了北京。大家集中工作了一个月的时间，把整个网络安全运行的标准规范、流程、操作规程、岗位职责、岗位技能要求等内容全部定义了出来。

“然后我们通过 9 月份的攻防演习和 10 月份的国际测试赛，再去验证这些流程策略、操作规程是不是能够走得通。一开始先是驻场的这几十人的演练，后来增加到 100 多人，最后到 300 多人。一遍一遍培训和演练的目的，就是为了让我们所有的参与者都熟悉相应的流程和操作规程。对于安全事件，无论谁在岗，他的处理结果都应该是一样的，不能因为人换了，处理的效果就变差。这是当时我们最担心的问题，因为人太多了。”

“担心”是尹智清这两年常常有的心情。按说，负责冬奥会网络安全整体规划，多是高屋建瓴的视角，但事实上，尹智清是大家眼里不折不扣的强迫症、细节控。

“每一个细节出问题都可能造成灾难性的后果，哪怕是一条配置指令写错。我们在做防火墙策略梳理的时候，看到很多防火墙策略中有 any，这意味着防火墙的策略控制不够精准。这是因为在整个建设过程当中，需要不停地调整策略，在调试的过程中很容易增加 any 用于测试，调整结束后，就忘了撤下来。我们在系统中部署了上百台墙。后来我们差不多花了一个多月的时间，梳理每一种类型的防火墙的策略，一条一条的梳理。这一条为什么存在，它的存在是否合理，这条和下一条的关系是什么？哪怕你一条配错，都是隐患。”

在反复的演练中，常态化运营也逐步深入人心。

推运营，稳扎稳打

常态化运营和重保相对应。冬奥是不是就是一个“大号”的重保？

尹智清觉得二者不能简单划等号。

“原来的很多重保停留在网络安全攻防演习或者是一种应对模式。这种思路会导致你会只关注到攻防层面的东西。但事实上如果真的是 APT 攻击，尤其是长期潜伏性质的，它会有很多蛛丝马迹。如果用强对抗的模式来分析，会漏掉很多内容，只能是设备告警了，你才能看到。如果攻击是用免杀或者是更隐秘的手段，安全设备可能不会告警。而系统日志、应用日志、流量等行为始终会有痕迹，但你平时可能会把这些细节忽略掉。回到奥运，我们要担负完全责任，不能忽略掉任何一个细节。所以冬奥采取的是常态化运营，所有跟安全相关的数据都集中在一起做分析。”

常态化运营的流程正是在一次次的演练中得以强化。

“以前大家习惯用一些攻防工具来做重保，强调局部分析，用 NGSOC 这种大数据平台去做安全运营的经验少。经过这一段的反复演练，到最后大家已经是完全熟练也非常习惯于用统一的安全运行平台来做安全分析。我觉得这是所有的驻场人员很大的一个进步。到 2022 年 1 月份的时候，整个流程已经比较顺畅，某种程度上已经变成一种机械式流程，也就是说让每个人都牢牢的记住，遇到什么事应该做什么样的操作。”

为保障冬奥会各项工作的信息网络安全，奇安信共计部署包括防火墙、天眼、天擎、椒图、上网行为代理、WEB 应用防火墙等在内的各类安全设备近千套，800 多个日夜、300 多名安全运行值守人员，每天处理超过 40 亿条各类网络安全相关日志，并对其中产生的数百条告警信息深入细致研判，在最短的时间内实现对安全事件的检测和响应，基于大数据建模，并对未来的安全趋势进行精准预测。

冬奥安全保障团队在北京冬奥会和冬残奥会组委会技术运行中心合影

冬奥会闭幕当晚，在奥组委驻守的奇安信同事们

挑大梁，不辱使命

800 多天的准备，经历了两次测试赛、两次技术演练检验、十轮次网络安全攻防演习，以及数不清的推演……所有保障人员迎来了最终的检验时刻。

冬奥开幕当天，尹智清等三个值班副经理都在 TOC（技术运行中心）。他们从 2019 年 12 月 26 日开始就一直驻扎在 TOC，日常分了三个班，轮流值班。但那天三人都在，谁在家里也坐不住。大家盯着一些关键的数据，实时刷新，处于读秒级的高度戒备状态。

“虽然在这一刻之前我们有过很多次演练，对于整个的架构、技术体系、流程、规范，大家心里有数，但上届冬奥会开幕式出现问题的画面，任谁也不敢有丝毫的放松。我当时觉得时间变得很慢很慢。”

台上一分钟，台下十年功。物理时间和心理时间的差异，源于冬奥网络安全保障体系宏大复杂，还充斥着无数的细节。作为规划者之一，尹智清始终保持着极度的认真，甚至是敬畏。

同一时间，奇安信董事长齐向东和总裁吴云坤分别在奇安信冬奥网络安全保障指挥中心和中央网信办值守。奇安信的工程师们则在各奥运场馆、关键部门、重要企业中值守。所有奇安信人共同守卫着冬奥网络安全。

依托先进的大数据架构、分布式关联分析引擎、机器学习和可视化等技术，奇安信团队在两个小时内，不间断将近千套不同设备，万余台终端及操作系统、数据库系统、业务系统等产生的 1.1 亿条日志等信息，实时进行标准归一化、关联分析、行为分析，进行实时动态、可视化的呈现，对所有攻击行为与异常行为进行了预警

与处理，守卫着北京这座“双奥之城”，又一次呈现无以伦比的精彩。

这份精彩最终延续到了 3 月 13 日。奇安信提前规划、参与建设，以“ 内生安全”“ 经营安全”的理念完成冬奥设施安全标准的规划，打造了全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环的“六全防护体系”，全域式保障了冬奥网络安全。奇安信兑现了承诺：北京冬奥会、冬残奥会网络安全“零事故”！

促成长，精进不休

800 多天的历程，每天都有新的挑战，每天都能进步一点。冬奥安全保障工作对于每个参与其中的人，对于整个奇安信，都是一个成长的加速器。对此，尹智清感受尤其深。

“冬奥其实是首次把公司几乎所有的产品都用上去，所有类型的人都用上去。在这个过程中，有几件事很重要。第一是从技术层面上，联防联动实现了所有产品之间数据的打通；第二是从产品层面，此前我们有些产品有的功能还不够完备，而冬奥保障的需求倒推着我们产品的功能点不断提升。仅在 2021 年 8 月，我们就提了 200 多个功能需求；第三是从运营的层面，整个公司标准化的工作得到了大大提升；第四是从保障模式层面，一线、二线、三线团队联动来做保障的这种保障模式又提升了一个维度。”

离开冬奥赛场，尹智清又要奔赴一个新的战场，任公司军团管理委员会关基总体部总经理。

“军团”是奇安信的组织创新，其模式来自于谷歌和华为，是把平台技术专家、应用技术专家、产品专家、工程专家、销售专家、交付与服务专家全部汇聚在一个部门，缩短产品进步的周期。“军团”基于不同领域的实际业务需要、业务场景，把过去离散度高的组织架构进行拆分重组，减少了大量中间环节，能快速集结资源，确保生产力的集中输出，为客户创造价值。

“这正是冬奥遗产之一。冬奥就是我们自己做架构、做交付、做实施、做运营，所有的人自始至终都在一个团队里工作，这种模式的好处就是这几个环节勾连紧密互不脱节。”

“军团”将复制奥运网络安全保障经验，优先在关基运营单位，首选央企、部委等大型机构进行实施。“军团”将把市场、规划、方案、产品、技术、交付、运营、安全服务一体化，更好地适应、满足重要领域客户的新安全需求。

永不灭，初心如炬

“接下来的目标，我觉得就要把奥运整体化运营的思路通过‘军团’关基总体部转化出来，为其他更广大的客户去使用。因为我本身是做运营的，我 2018 年加入公司的时候就一直想把常态化标准化安全运行用于实战。这是我的一个心结，就是想把它再推广。”

冬奥驻守期间，尹智清在首钢园跑步

像尹智清一样，奇安信人跑完了自己的冬奥之路。他们书写历史，也成为历史的一部分。

而对于整个奇安信来说，公司在冬奥网络安全保障上收获了宝贵的实战经验，加速了多项研发平台的市场化及研发投入的成果化进程。“一起向未来，既是冬奥会与冬残奥会的口号，也是我们未来继续做好网络安全保障的目标。”奇安信集团董事长齐向东说。

“成为世界第一的网络安全公司”。奇安信离自己的梦想又近了一步。 安

她们｜冬奥背后的“奇女子” 诠释新时代的“女性力量”

作者 公关部 包世玉

国家十四年，实现了2008年奥运会到2022年冬奥会的传承，完成了中国GDP总值从4.6万亿到17.7万亿的跨越。

行业十四年，是从C端免费杀毒软件到B端冬奥网络安全保障全系统的转变，产业规模从十亿到千亿的扩张。

人生十四年，是从一个奥运观看者到冬奥工作者的转换，也见证了一个姑娘从青涩学生到成熟职场人的蜕变。

时代的浪潮奔涌向前，科技的力量蓬勃壮大。女性科技人才由2009年底的2160万人上升到2017年的3560.6万人，占科技人力资源总量的38.9%。2021年，女性占网络安全人才的比例接近1/4；奇安信的校招生中，有近1/3是女生。

在科技行业中，有越来越多的年轻女性加入、发挥自己的才能和力量。在奇安信，也有这样的一群“奇女子”，争分夺秒地保障冬奥网络安全，绽放她们独特的光芒。

“工作不分性别，我们都属于奇安信‘军团’。”

——当仁不让、独领风骚

“在20kg的设备面前，不分性别。”莎莎是冬奥保障中交付队伍的一员，她说在面试时面试官也曾问过她：作为一个女孩子，能够胜任交付工作吗？莎莎说：“技术上当仁不让。如果只是设备搬不动，我就去健身，只要想，这都不是问题。” 这个回答让面试官一下子就记住了她这个与众不同的女孩子。

在北京零下十几度的冬奥战场上，奇安信就拥有这样一群“奇女子”，她们认真对待工作、认真对待生活，巾帼不让须眉。

“春节没回家。”98年的校招生雯雯想到这是自己第一次不能回家过年，多少有些哽咽，“但想到这里是各国运动员进入中国的第一关卡，心中的责任感和使命感也是满满的！”1月1日，正值元旦假期，雯雯听说场馆需要一个人提前进入闭环进行场馆部署，毫不犹豫地接下了任务。作为一个女孩子，提前进入闭环，不说设备沉重，里面也没人照应，领导多少也有些担心。但短短3天，雯雯在2日飞抵北京、确认方案、沟通实施工作，3日入住闭环、搬行李、学习穿脱防护服，4日，上架、部署、联调，她以绝对的速度和专业的水准圆满完成任务。

这次奇安信在“国门第一关”——首都国际机场闭环内驻守的，除了雯雯，还有来自北方的姑娘笑源。雯雯坦言：“时不时需要穿上闷热的防护服在场馆内工作，行动不便不说，风险也是有的。”但两个人一起工作生活，互相照应，笑源活泼开朗的性格让两人在闭环内的日子充满了乐趣。

若说对一线的照应，就不得不提起负责冬奥后勤工作的小霞和聪聪。两位姑娘因为为一线提供衣食住行的保障，被大家戏称为“三头六臂的哪吒”。

其实要说她们是“三头六臂的哆啦 A 梦”都不足为过。从 1 月开始到现在，两人共处理了 200 多个采购单、与几十家酒店签合同付款、准备出所有前线同事的物资、组织值守同事每天做核酸，从早忙到晚，有求必应。即使休息期间也是 24 小时开机，一旦有需要，随叫随到。

在得知有同事的住处条件艰苦时，两位姑娘就立刻采购了一系列生活用品：从电暖气、棉被、热水壶、暖宝贴，到饮用水、泡面、自热饭，为大家一一备齐。“几个月都没有休息过，现在已经习惯了。行政的工作事无巨细，但也有它的乐趣所在。用我们的付出，保障前线同事安心工作，这就是我们行政工作的价值所在。”

“行业中女孩子越来越多啦！我们自然有自己的优势。”

——以柔克刚、不卑不亢

时代变了，网络安全行业也需要女生。

“从来没觉得领导在工作中有任何偏颇。”金凤是驻守在北京颁奖中心的另一位“奇女子”，这个场馆里只有她自己一个人身处闭环内。在圆满完成冬奥保障工作的同时，她也见证了中国首金。提起谷爱凌，金凤说当她夺冠时自己激动坏了：“谷爱凌太火了，我对她印象很深。”在保障工作中，金凤说基本没有遇到过任何阻力，“冬奥期间，每天工作时都会想起谷爱凌，深受鼓舞。她让我更加觉得，女生只要有能力、有自信、有想法，工作中的压力反而是动力。”

“距离冬奥开幕式还有 96 小时的时候，我们接到了奥组委需要新增一整个模块的需求。”奇安信态势感知负责人常月接到了棘手的任务。当时的她心里一紧，又是一个硬骨头。接到任务后又不得多想，她立刻协调各方资源，快速进行产品版本设计、开发。常月带领团队按照每 24 小时进行一个版本迭代的速度，共迭代了三个版本、更新了 100 多个小功能。最终在奥运会临开幕前，成功将新模块在 2 月 3 日晚上正式发布上线。以神速完成了这个看似不可能完成的任务，这位“奇女子”一战封神。

“一个女孩子，学技术不太好吧。”雯雯提起自己入行网络安全，确实是有不少故事可谈。“我最开始学的是食品安全，学了之后觉得不适合自己，便转专业到一直感兴趣的信息工程专业。再后来接触到了网络工作，就报名了网络安全的课程自学。” 雯雯说，转专业时周围不少人都有疑议，但她毅然决然地坚持在这条路走下去。“其实女生有自己的优势，细致、耐心，善于沟通，在工作中收到的表扬信不少。自己也经常从身边的优秀女性中得到力量。”在雯雯刚入职时，几十号人里女孩子只有三个，到现在，女生越来越多了，这次雯雯驻守冬奥队伍的五人中就有三个姑娘。

行业内的“奇女子”也越来越多，细心细致、以柔克刚、不卑不亢，她们在用自己的优势实现行业的抱负。

“妈妈是我的‘奇女子’，她的支持让我充满力量。”

——相互扶持，自信传承

“妈妈收到公司寄给冬奥工作同事的关怀礼盒时感

动哭了。第二天化上妆，激动地戴上围巾给周围人看，可自豪了。”小霞提起自己的妈妈，语气中充满了敬佩：“我妈妈是个女强人，赚钱的事情从来都往前冲，从小拉扯我们姐妹三个长大。在亲戚劝母亲考虑不要让我们三姐妹读书时，妈妈也是一直都没有同意。”小霞因为冬奥后勤保障的工作，已经很久都没能回家了，但妈妈却一直很支持小霞的工作。

行政的工作总是充满了细微琐事，在冬奥期间起早贪黑连轴转了几个月，难免遇到一些不如意的事情，但小霞说：“是妈妈的正能量，让我在工作中一直保持着积极的心态。她为了我们姐妹三人，一直在力所能及的范围内努力工作，虽然辛苦，但她从未抱怨。看着妈妈的经历，让我知道，无论是什么工作，只要热爱，你就会是那个发光的人。”

不要给自己的人生设限，要永远积极地尝试。在雯雯想要从食品专业转到通信工程时，她说：“妈妈一开始没有说话，但我妈妈在网络上查找了好多资料，最后打电话跟我说，想做的就去放手做吧，妈妈支持你。”雯雯说，自己的妈妈就是这样一个开明、勇于尝试的女性，从小到大，她给了雯雯很多启发。“记得小时候妈妈因为要做淘宝，就自己装系统，攒电脑。厉害极了。”雯雯提起这些，眼中充满了崇拜，可能就是这样的妈妈，以身作则，言传身教，让雯雯从小感受到了科技的神奇，冥冥之中，让她也走上了网络安全的道路。“没有妈妈的启发，可能曾经的我就不会有勇气转到这个行业中，今天的我就不会有机会加入到冬奥的工作，也不会有机会随着行业的大势快速成长。说起来，她才是我的‘奇女子’！”

在网络安全领域，男性从业者往往占据大半江山。“只要做正确的事，就不畏艰险！” 这是常月经常挂在嘴边的一句话。常月作为众多的“程序媛”之一，一直积极探索利用新技术，成功将态势感知推向一个全新的高度。今年过年期间，因为冬奥的工作，常月陪伴女儿的时间很少，但好在公司设立了“家属开放日”，常月的女儿安安如愿来到奇安信大楼和妈妈一起“上班”。摸着公司一层的乐高虎符，安安眼中充满了好奇。虽然，先进的乐高技术理念在孩子眼中还只是玩具，但未可知，可能就是这一次随妈妈的“探险”，在她心中埋下了那颗想要成为“奇女子”的种子。

在冬奥战场英姿飒爽，在网络安全行业当仁不让。正是这样的一群“奇女子”，以她们的方式展示着自己的力量。

休言女子非英物。十四年，成长、传承，是女性群体的蜕变，也是女性力量的迸发。

未来，行业、国家，或许更多女性得以其柔和之姿，展现出她们独特的力量与光芒。 安


"零事故"精神，就是担当精神
网络安全 中国代表队 奇安信

3 月 20 日下午，奇安信召开网络安全中国代表队表彰大会暨集团年会，迎接开创网络安全“零事故”奥运历史的奇安信冬奥将士凯旋。

听说周报写 5000 字就能升职加薪？不存在的！

作者 公关部 王梦琪

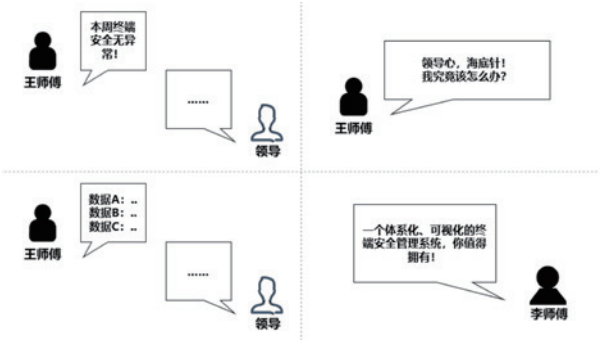
01 写周报引发的思考？

“洛阳亲友如相问，就说我在写周报”“黑发不知勤学早，周报怎么能写好”“垂死病中惊坐起，打开电脑写周报”……如果靠近这个双眉紧皱、紧盯着电脑的中年男子，就能听到他口中不断的碎碎念。

王师傅是某金融集团网络安全部终端安全负责人，周围同事对王师傅这幅样子早已见怪不怪了，这种画面每周五都会上演。显然，王师傅又被这周的周报难住了。

整个集团包括各个办公地点加起来，有上万台型号各异、新旧不一的终端，这些终端直接关系着公司内外网安全情况，王师傅团队每周经手处理的日志数据量十分庞大，打补丁、杀病毒、运营维护等日常工作也非常烦琐。但偏偏就是这样充实的工作日常，难住了王师傅汇总工作周报。

在王师傅看来，自己日常工作落实在周报上，千言万语只有一句话：本周终端安全无异常。后果可想而知，王师傅被领导怒喷两小时后被责令整改周报内容。这次王师傅选择将各类数据都汇总进去，详尽展示本周终端安全运行的情况。面对一堆挤在一起、摸不清重点的数据，王师傅的领导长叹一口气，努力从中提炼出自己想要的信息。



怎样才是领导最想看到的周报？为此，王师傅拉了几个熟悉的同行一起吃饭，主要还是想取取经。同为企业终端安全负责人，另一位李师傅就在工作中如鱼得水，不仅连续获得高绩效，还被评为年度优秀员工。

关于困扰王师傅许久的难题，李师傅一语道破关键——

“周报难，难在你还总停留在安全工程师的杀病毒、补漏洞等技术思维，缺少管理思维和运营思维。”

02 李师傅的成功秘籍？

很多公司都有月报、周报、日报的汇报机制，为此涌现了一大批文笔动人、篇幅感人、格局惊人的周报“卷王”。实际上，李师傅认为写好周报十分关键，一方面，领导需要从中掌握项目态势，随时动态调整，优化工作过程，实现整体目标；另一方面，也代表着自己对工作内容的掌握与思考。尤其是网络安全相关的工作，更需要通过汇总报告，传递安全状况、呈现安全态势。

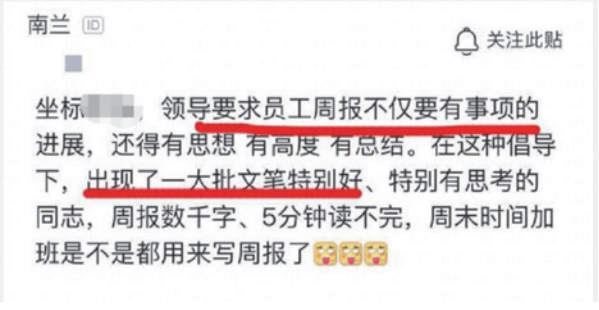
李师傅总结了周报的两个误区。

误区 1：内容干瘪 分析不足

“无安全事故”，无疑是网络安全人员追求的目标

和 KPI。可是，它既体现不出安全人员在幕后付出的专业技能和辛苦劳动，也无法让 IT 部门、业务部门和企业管理者、监管部门等看到中间的过程分析，如风险情况、薄弱环节、合规落实情况，以及有价值、感兴趣的核心信息，这样的周报显然不合格。

实际上，终端安全的范畴，早已超越了早期的木马、杀毒和补漏洞范畴，安全配置、漏洞补丁管理、软件安装合规性，外接设备、移动存储数据交换、非法外连行为、隐私保护等，都是终端安全的范畴。如果文字太短、内容泛泛、信息太少、缺少体系化的分析，就无法让领导和其他部门有全局、清晰的了解。



误区 2：长篇大论 华而不实

当然，因为终端安全工作琐事繁多，是否可以事无巨细、长篇累牍的汇报安全工作呢？其实，其他部门和领导的时间，都是有限和珍贵的，如果文字过长、辞藻华丽、注重形式，领导既没耐心也没时间提炼重点，也只是出力不讨好。

那么，如何写一份好的周报呢？李师傅认为，一定需要有管理视角和运营视角，站在协同部门如信息化部门、业务部门，以及企业管理者的视角，并且清晰呈现关键信息。

无论是报平安的简单概括，还是常规的各维度数据罗列，显然，这都不是上级最想知道的。从管理者和运营的视角出发，终端安全难在如何强化管控、杀毒、漏洞补丁等各种安全防护手段，难在如何从海量、多维度的终端数据中精准发现潜在威胁，掌握整体安全态势。

简单来说，如何有效利用在终端运营、维护过程中产生的数据，从而对企业安全运营工作起到积极的影响，对企业安全管理来说至关重要。

在管理者眼中，数据意味着可度量、可优化，没有清晰的数字指标，管理者难以清楚掌握整体终端安全态势，更不会知道自己的薄弱点在哪里？有多少潜在风险？安全风险在运营过程中增加了还是降低了？而有了清晰的数字指标，管理者就可以以此来驱动安全运营的优化，最终提升安全管理效果。

李师傅所在的企业引进了奇安信天擎终端安全管理系统（简称天擎），采用天擎数据可视化系统（简称可视化系统）搭配终端安全运营平台（简称安运平台），构建“体系化防御、数字化运营”能力，这也正是李师傅无惧周报、高效协同的制胜武器。

03 天擎能解决什么问题?

李师傅认为，周报直接体现了汇报人的能力水平。这里的能力是指发现问题、解决问题的能力，以及将目标转化为任务的能力。那么在这一点上，天擎都解决了什么问题呢?

首先，天擎能够全面、清晰地展示数据维度，让整体安全态势一目了然。

可视化系统 + 安运平台的组合，不仅为李师傅直观展现了漏洞事件、安装部署、病毒事件、违规外联、资产概况等十四大维度威胁情况，还可直接根据李师傅所在单位的需求定义可量化的终端安全指标。这样一来，李师傅的周报维度清晰、目标突出，还成为了领导心中十分认可的运营、分析工具和决策支持。

其次，天擎解决了终端安全数据可视化、可量化的问题。

数据可量化，意味着李师傅可以将终端数据直接转化为工作任务，围绕整体目标进行调整，并且团队工作过程也随之可优化、可调整。李师傅的领导也可以根据动态运营情况有效地部署，实时调整整体终端安全策略，真正做到高效、可见的安全运营。

最后，天擎解决了漏洞补丁管理难题，充分解放运营人员。

对于终端安全负责人来说，漏洞怎么处理、补丁该不该打等问题，始终是管理痛点，而有了天擎之后，李师傅可以第一时间掌握漏洞分布情况，并基于安全策略和处置优先级，给终端及时打上最新补丁。在整体环境日益复杂的情况下，李师傅觉得，天擎明显改变了以往追求“操作规范”而难以招架的情况，将终端安全变成“效率优先”。

在李师傅看来，天擎主要解决的这三大核心问题，让自己的周报既有全局态势，又能清晰展现各重点维度数据，并且工作目标清晰，优化改进方向明确，为领导安全管理决策提供了重要支撑，这也正是李师傅从来不为写好周报发愁的重要原因。

俗话说：周报写得好，加薪跑不了。在听过李师傅的介绍后，王师傅终于拨开云雾领会到了领导的需求到底是什么，也更加迫不及待想见识一下奇安信天擎的功能与可视化数据展示。

可以说，也正是奇安信天擎所构建的“体系化防御、数字化运营”能力，不仅让李师傅深受领导赞赏，也让整个终端安全在公司的地位大幅度提升，成为公司举足轻重的部门。有了李师傅分享的经验之谈，相信王师傅很快也能摆脱周报带来的烦恼！ 安

大事记

奇安信圆满完成北京冬奥会与冬残奥会网络安全保障任务

“奇安信圆满完成北京冬奥会、冬残奥会网络安全保障任务，兑现了‘零事故’承诺！”2022 年 3 月 13 日晚，2022 年北京冬残奥会落下帷幕。奇安信作为奥运史上首家第三方网络安全服务商，交上了北京冬奥会、冬残奥会网络安全保障“零事故”的满分答卷。

据奇安信冬奥网络安全负责人介绍，为保障冬奥网络安全“零事故”，奇安信先后投入 3500 多名专家，首次系统性、全局性进行网络安全规划，统筹部署冬奥网络安全保障工作。并由集团董事长齐向东亲自担任总指挥，成立 11 支团队进驻一线；807 名员工在二线值守；启用冬奥网络安全应急热线 95015。部署网络安全设备 55款 813 台，涉及三个赛区 38 个场馆和 188 个服务场站，覆盖终端超 10000 台。同时，为涉奥的政府部门、运营商、电力等 145 家重保单位提供现场防护服务。

冬奥“零事故”经验宣讲团成立大会召开

3 月 16 日，冬奥网络安全零事故经验宣讲团在京正式成立，奇安信集团总裁、奇安信冬奥网络安全保障副总指挥吴云坤担任宣讲团团长，华北电力大学教授、博士生导师李建彬等 7 位长期深耕在网络安全行业的知名专家教授担任外部专家，以及奇安信安全专家一起，共同组成冬奥网络安全零事故经验宣讲团。

北京冬奥会和冬残奥会组织委员会技术部副部长贾力提出，希望通过冬奥网络安全“零事故”经验宣讲团，对冬奥网络安全保障工作进行全面准确梳理、认真扎实总结、精彩鲜活传播，为数字中国保障提供经验。

冬奥网络安全卫士总结表彰大会在奇安信召开

3 月 16 日，冬奥网络安全卫士总结表彰大会在奇安信冬奥网络安全保障指挥中心召开。来自国资委、国家

优秀冬奥网络安全卫士所属单位/平台	
中国核工业集团有限公司	中国电信集团有限公司
中国航天科技集团有限公司	中国联合网络通信集团有限公司
中国航天科工集团有限公司	中国移动通信集团有限公司
中国航空工业集团有限公司	中国卫星网络集团有限公司
中国兵器工业集团有限公司	中国电子信息产业集团有限公司
中国电子科技集团有限公司	中国航空集团有限公司
中国石油天然气集团有限公司	中国东方航空集团有限公司
中国石油化工集团有限公司	中国南方航空集团有限公司
中国海洋石油集团有限公司	中国交通建设集团有限公司
国家石油天然气管网集团有限公司	中国民航信息集团有限公司
国家电网有限公司	中国广核集团有限公司
中国南方电网有限责任公司	中国医学科学院阜外医院
中国华能集团有限公司	北京大学第三医院
中国大唐集团有限公司	四川大学华西第二医院
中国华电集团有限公司	江苏省人民医院
国家电力投资集团有限公司	潍坊市中医院
中国长江三峡集团有限公司	华中科技大学同济医学院附属协和医院
国家能源投资集团有限责任公司	补天漏洞响应平台
鹏城实验室	

卫健委、29家央企及鹏城实验室等单位的“冬奥网络安全卫士”做出突出贡献，获得表彰。

北京冬奥会期间，经过层层选拔的冬奥网络安全卫士24小时在线，发起超过2000万次测试请求，测试总时长超过1万小时，成功发现了大量有效的系统漏洞和冬奥相关的威胁情报。

奇安信集团副总裁韩争光受聘为工联众测平台特邀专家

3月14日，由中国工业互联网研究院建设的“工联众测平台”正式上线试运营，并陆续公布了特聘专家的名单。奇安信集团副总裁、奇安盘古CEO韩争光受聘为首席特邀专家。

作为平台首批特邀专家，韩争光未来将为平台提供战略性、前瞻性业务指导，推动工业互联网企业安全能力建设，促进工业互联网安全防护发展的同时，充分输出盘古在安全领域的能力和研究成果，赋能国内更多的政企用户，为保障人民安全、社会安全、国家安全，添砖加瓦，做好数字时代下网络安全的守护者。

北京市委统战部部长游钧一行到访奇安信调研冬奥网络安全保障工作

3月7日，北京市委常委、统战部部长游钧，副部长、市工商联党组书记赵玉金走访奇安信集团，调研北京冬奥会、冬残奥会网络安全保障相关工作。

对奇安信“零事故”完成冬奥网络安全保障的成绩和贡献，游钧表示肯定，并对奇安信创新“中国模式”、采用“中国架构”、研发“中国产品”、部署“中国服务”的创新意识和能力表示赞许。

游钧指出，网络安全事关社会经济发展、国计民生，未来发展的空间和潜力都是巨大的，希望奇安信积极面对挑战，坚持创新、开拓，及时总结冬奥网络安全保障工作的成功经验和模式，继续做好冬残奥网络安全重保，并在未来的工作中进一步推广应用。同时，他希望奇安信持续发挥“隐形冠军”的技术和行业优势，在创新攻关、非公企业党建、践行企业社会责任等方面，在民营企业中作标杆示范。

奇安信公益基金会为援港抗疫捐赠20万只KN95口罩

3月1日，首都统战各界人士援港抗疫捐赠仪式在京举行。奇安信公益基金会积极响应援港抗疫的号召，向香港社团捐赠20万只KN95防护口罩，为香港民众打赢第五波疫情防控阻击战提供支持。

新冠疫情爆发以来，奇安信一直积极践行企业社会责任，奔赴在抗疫前线。为更专业地践行企业社会责任，经北京市民政局指导和批准，2021年10月9日，奇安信集团出资设立的“奇安信公益基金会”正式成立。

基金会以开展慈善活动为宗旨，不以盈利为目的，设立健康助医、灾害救助、教育助学和扶贫助农四大工作领域。

奇安信发布 2021 漏洞态势报告：重点漏洞数量急剧上涨

近日，奇安信 CERT 正式对外发布了《2021 年度漏洞态势观察报告》（简称《报告》），围绕漏洞监测、漏洞分析与研判、漏洞情报获取、漏洞风险处置等方面描绘过去一年全网漏洞态势。

《报告》显示，2021 年奇安信 CERT 新收录漏洞信息 21664 个（其中 20206 条有效漏洞信息在 NOX 安全监测平台上显示），经 NOX 安全监测平台筛选后，有 14544 个敏感漏洞信息触发人工研判，其中 2124 个漏洞影响较大，触发了奇安信 CERT 的应急响应流程。据奇安信 CERT 负责人介绍，相较于 2020 年，触发应急响应流程的漏洞数量增长了 150% 以上。

北京 2022 年冬奥会网络安全“零事故”经验总结研讨会在奇安信召开

2 月 21 日，来自北京冬奥组委、科技冬奥重点专项项目组及奇安信集团负责冬奥网络安保的相关专家在奇安信安全中心召开“北京 2022 年冬奥会网络安全‘零事故’经验总结研讨会”，对冬奥网络安全保障工作、“科技冬奥”专项项目实施情况进行了总结汇报，同时按冬奥组委技术部要求启动经验总结工作。

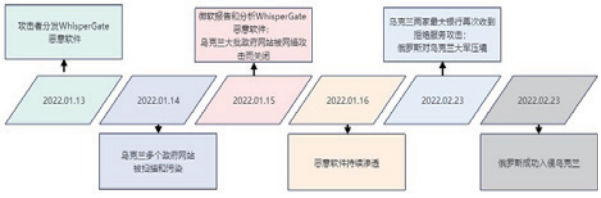
“科技冬奥”重点专项项目负责人表示，该项目提升了冬奥赛事网络中现有安全检测和防护平台进行防护能力，在标准规范、工具专利等方面取得了一系列进展，基本完成了项目中期计划指标。

奇安信集团董事长、奇安信冬奥网络安全保障总指挥齐向东对各位领导、专家在冬奥网络安全保障过程中提供的支持和帮助表示感谢，同时表示，奇安信将按照北京冬奥组委技术部的要求，尽快进行工作经验的梳理和总结，使其能够服务于建设现代化国家的目标。

独家披露！奇安信发布针对乌克兰目标的系统破坏攻击分析

2022 年 2 月 24 日，随着俄乌冲突不断升级，俄罗斯总统普京宣布对乌克兰部分地区进行特别军事行动。实际上，在特别军事行动之前，大规模的网络战争已经提前发动。奇安信威胁情报中心、技术研究院在第一时间对外披露，以乌克兰政府、金融等系统为目标的破坏攻击完整分析报告。

分析报告对乌克兰近期遭遇的数据擦除攻击和 DDoS 攻击的时间节点、技术细节、恶意影响等进行了完整还原和深度解析，尤其对擦除数据的“恶意幽灵”，进行了详细的样本分析、攻击载荷、追踪溯源，并通过司南平台对本轮 DDoS 攻击的受害网站分布、攻击流量趋势、攻击细节等进行了分析还原，对外展示了网络战的典型作战方式。目前，奇安信天擎终端安全管理系统已经支持以上两项攻击样本的查杀。



北京奇安盘古实验室发布报告 揭露美国安局顶级后门“电幕行动”

2 月 23 日消息，北京奇安盘古实验室科技有限公司发布报告，披露了来自美国的后门——“电幕行动”（Bvp47）的完整技术细节和攻击组织关联。这是隶属于美国国安局（NSA）的超一流黑客组织——“方程式”所制造的顶级后门，用于入侵后窥视并控制受害组织网络，已侵害全球 45 个国家和地区。

报告显示，“电幕行动”（Bvp47）在全球已肆虐十余年，广泛入侵中国、俄罗斯、日本、德国、西班牙、意大利等 45 个国家和地区，涉及 287 个重要机构目标。其中日本作为受害者，还被利用作为跳板对其他国家目标发起攻击。相较一般的 APT 攻击手段，“电幕行动”堪称顶级后门程序，可以让“方程式”组织在网络空间里畅通无阻，隐秘控制下的数据获取如探囊取物，在国家级的网络安全对抗中处于绝对的主导地位。

荣誉墙

奇安信入选首批信创政务产品安全漏洞专业库技术支撑单位

近日，国家工业信息安全发展研究中心公布首批“信创政务产品安全漏洞专业库技术支撑单位”名单，奇安

信网神凭借在信创领域的漏洞发掘、应急响应、处置服务等方面的综合能力成功入选。

信创政务产品安全漏洞专业库（简称“信创漏洞库”，英文简称 CITIVD）是国家工业信息安全发展研究中心为贯彻落实《网络产品安全漏洞管理规定》的要求，在工业和信息化部网络安全管理局组织指导下，建设和运营的针对信创政务产品安全的专业漏洞库。

奇安信与人保财险合作案例入选网络安全保险新业态新模式十大典型案例

3 月 9 日，国家工业信息安全发展研究中心发布了“2021 年网络安全保险新业态新模式十大典型案例”，由人保财险和奇安信申报的“医疗行业网络信息安全保险案例”成功入选。

奇安信相关负责人表示，作为网络安全厂商，奇安信希望依托自身的安全服务和技术优势，破解保险业在网络安全方面的准入难问题，为网络安全保险产品创新、业态发展提供技术支撑。

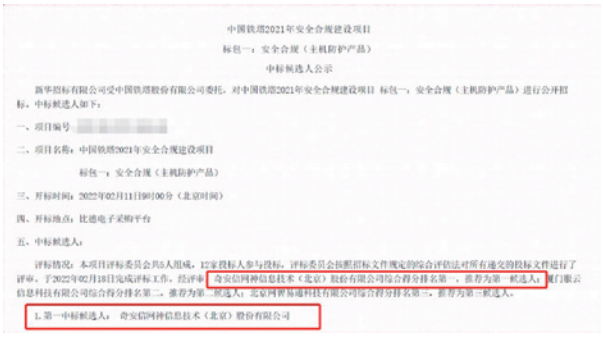
奇安信斩获 CSA 2021 安全磐石奖 彰显全栈云安全能力

3 月 9 日，第六届云安全联盟大中华区大会（CSA GCR Congress）上，奇安信成功斩获 CSA 2021 安全磐石奖，充分彰显了其全面、立体的一站式全栈云安全能力。

CSA 2021 安全磐石奖是云安全领域年度最具含金量的奖项之一，代表着获奖企业具备较强的组织安全能力和防护体系，有效解决企业或用户在新型网络环境中安全问题的综合解决方案，给业内提供良好的参考价值及引领作用，综合实力强，影响力广，有效促进社会及城市数字化转型。

排名第一！奇安信中标中国铁塔安全合规项目

近日，中国铁塔公布了 2021 年安全合规建设项目标包一——安全合规（主机防护产品）的中标候选人名单。



奇安信集团旗下网神公司以综合排名第一的成绩，成为该项目第一中标候选人。这也是奇安信继连续中标中国电信、中国移动、中国联通集采之后，在通信行业主机安全领域的又一大突破。

经过多轮的评审和综合比较，奇安信提供的以椒图为核心的主机安全防护产品，凭借“漏洞利用防护”“应用运行时自我保护”“微隔离”“攻击溯源”等全面的主机安全核心能力，以及覆盖主机安全“预测 – 防御 – 监控 – 响应”全链条的自适应安全标准，获得了客户认可，最终以综合排名第一的成绩成为中标候选人。

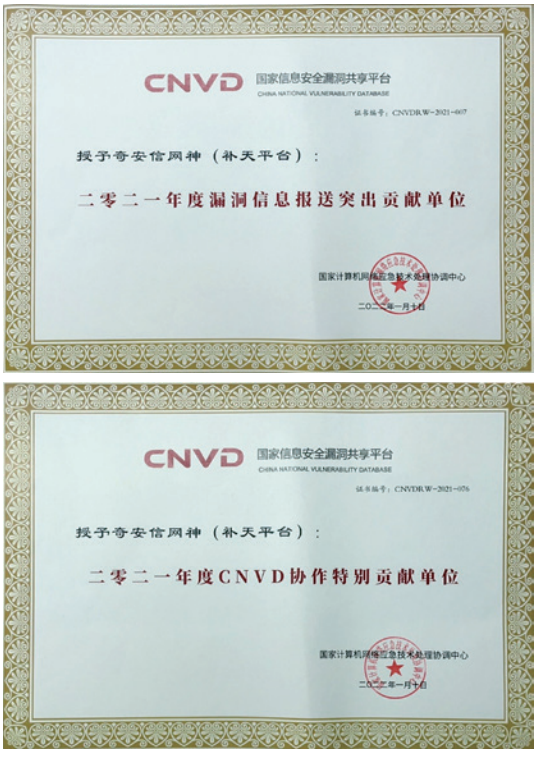
实力领先！奇安信安全访问服务（Q-SASE）斩获金智奖

近日，由信息安全与通信保密杂志社主办，中关村智能终端操作系统产业联盟协办的 2021 年度（第六届）“中国网络安全与信息产业金智奖”评选结果公布，奇安信集团参选产品“奇安信安全访问服务（Q-SASE）”脱颖而出，斩获“优秀产品”大奖。

奇安信安全访问服务（Q-SASE）是在 Gartner SASE 架构基础上结合国内网络安全现状及奇安信自身优势能力，应运而生的一款解决方案级服务化产品。Q-SASE 以“软件定义网络 + 软件定义安全”为技术路线，通过将网络和安全能力融合为统一的服务，实现了互联网应用（向外）、内网和私有云应用（向内），以及远程办公等兼顾良好体验和安全效果的高质量访问，解决了多级多分支企业安全边界模糊、安全能力分散、安全运营投入高效率低以及难以支撑集团“体系化、实战化、常态化”的安全防护体系建设和安全运营要求的业界难题。

奇安信荣获 CNVD 漏洞信息报送突出贡献单位等多项荣誉

在 23 日召开的国家信息安全漏洞共享平台（CNVD）2021 年度工作会议上，奇安信网神信息技术（北京）股份有限公司旗下的补天平台，获得“2021 年度漏洞信息报送突出贡献单位”“2021 年度 CNVD 协作特别贡献单位”称号，补天平台多名精英白帽入选年度十强白帽和优秀个人，同时，奇安信网神被 CNVD 认证为“CNVD 技术组支撑单位”。



奇安信位居“2021年中国网安产业竞争力50强”第一名

6月16日，中国网络安全产业联盟（CCIA）揭晓
“2021年中国网安产业竞争力50强”。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信位居第一名。

“2021年中国网安产业竞争力50强”榜单

TOP15	公司名称	公司简称
1	**奇安信科技集团股份有限公司**	**奇安信**
2	深信服科技股份有限公司	深信服
3	启明星辰信息技术集团股份有限公司	启明星辰
4	华为技术有限公司	华为
5	天融信科技集团股份有限公司	天融信
6	腾讯科技(深圳)有限公司	腾讯
7	阿里云计算有限公司	阿里云
8	新华三技术有限公司	新华三
9	绿盟科技集团股份有限公司	绿盟科技
10	杭州安恒信息技术股份有限公司	安恒信息
11	三六零安全科技股份有限公司	三六零
12	亚信安全科技股份有限公司	亚信安全
13	中孚信息股份有限公司	中孚信息
14	杭州迪普科技股份有限公司	迪普科技
15	山石网科通信技术股份有限公司	山石网科

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

“零事故”

奇安信圆满完成冬奥会网络安全保障任务