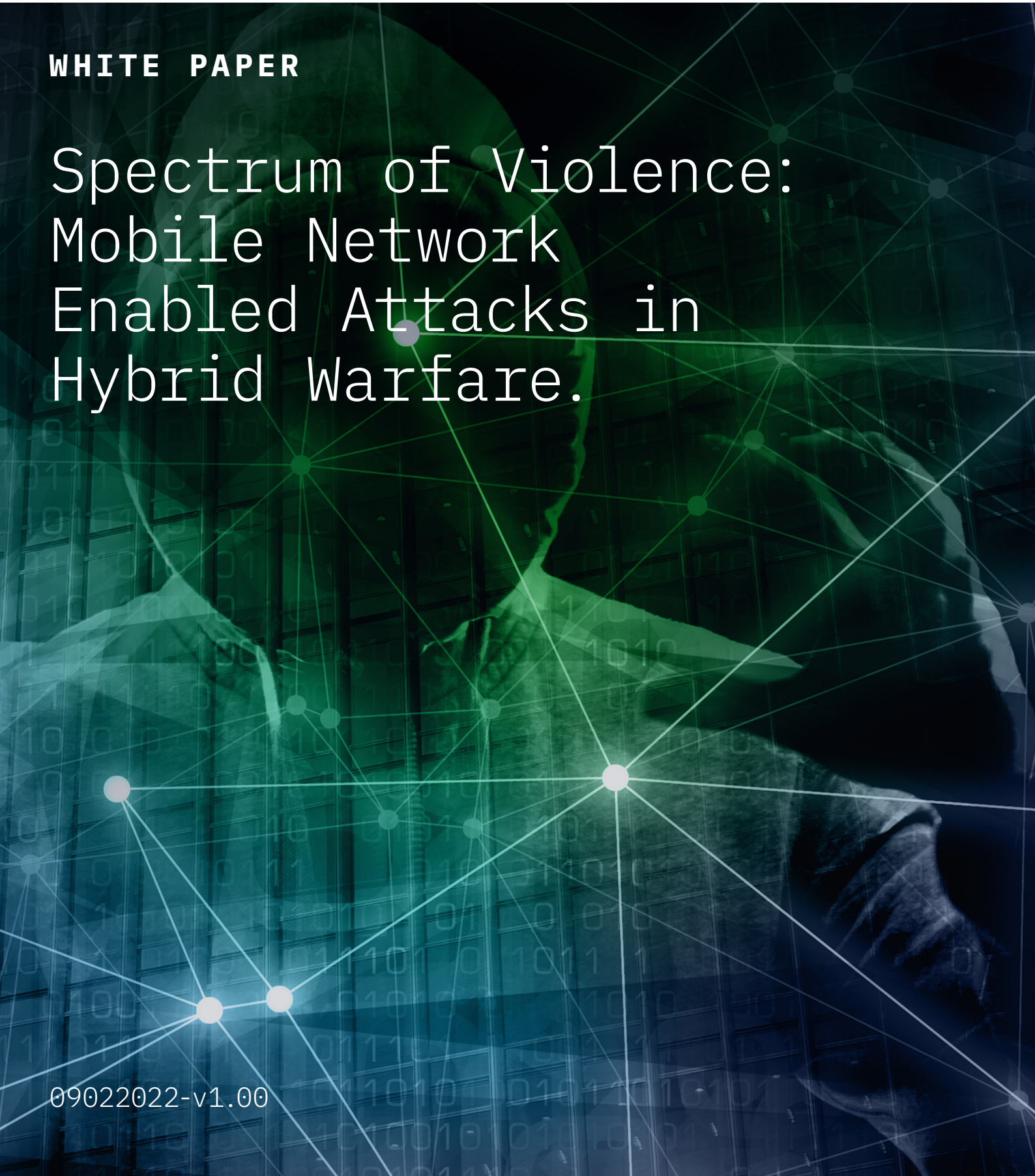
AdaptiveMobile Security
an Enea company



WHITE PAPER

Spectrum of Violence: Mobile Network Enabled Attacks in Hybrid Warfare.

09022022-v1.00

Legal Notices

Revision History

Revision	Date	Remarks
1.0	09/02/2022	Release version

Revision	1.0

Table of Contents

1 Introduction

Much research and reporting has been focused on the conduct of cyberwarfare in the context of military operations. Focus on the topic has certainly been merited especially since states began to introduce cyber force concepts to military services in the 2000s[1]. While real-world instances of cyberwarfare – understood as the use of cyber operations specifically to destroy or disable a target to further political objectives (as distinct from cyber espionage or cybercrime) - have been comparatively few in number, the costs inflicted, and the danger posed even by limited cyberwarfare campaigns is increasing[1]. At this time of heightened tension in the Euro-Atlantic region, understanding the modalities and implications of cyberwarfare is more vital than ever before.

A widespread recognition of the prominence of the use of cyberattacks as part of broader "hybrid threat operations"[2] aimed at manipulating the information environment in Europe has focused the attention of many on attacks against the I.T. networks of critical installations and infrastructure. There has been limited reporting of destructive cyberwarfare attacks aimed at disrupting telecom network services.

To date however, no report has covered how **attacks enabled by the weaponization of the functionality of mobile telecom networks** could achieve objectives within the battlespace as a hybrid threat vector and 'force multiplier' for offensive military measures.

In this white paper we will first give an introduction on what hybrid warfare is, and the role that cyber-attacks play in it. We will then give an overview of an increasingly critical component of cyber warfare – telecom networks - and specifically mobile telecom networks, describing the types of threats encountered on these networks today. We also announce our identification of an advanced complex platform that uses mobile network infrastructure globally that we have called: **HiddenArt** – a mobile Advanced Persistent Threat (APT).

This paper will then outline two use cases among the many possible in order to illustrate how attacks on mobile networks might be executed in the event of an offensive military campaign. To help shine further light on the potential threat posed, we will share observed offensive and defensive activity in this space.

Finally, we will outline a list of recommendations that mobile operators, regulators, government agencies and other stakeholders should act upon in order to ensure that their critical communication network infrastructure is safe from attacks by Organized Crime Groups (OCGs), Surveillance Companies and State-level Threat Actors.

AdaptiveMobile Security make this attack model and our identification of the HiddenArt mobile network threat actor public with the aim that drawing the attention of the international community to the potential threat presented might deter any such attack activity. We also aim to contribute to deeper discussions internationally of the increasingly profound implications of extant vulnerabilities in insufficiently-protected mobile network infrastructure for the security and stability of societies, economies, and states into the future.

2 Hybrid Warfare and Telecommunications

Recent writing[3] on the subject of 'cyber surprise' attests that defenders tend to be "routinely staggered" by cyberattacks despite having acknowledged the possibility beforehand. This is due to some inevitably unforeseen element of intensity, impact, timing, trend, means, or target itself that renders the attack both expected and yet surprising in manifestation.

At this time of heightened concerns over the possibility of a new Russian invasion of Ukraine, the many modalities, conventional and unconventional, that may come into play are the subject of intense discussion and speculation throughout Europe and around the world. A destructive cyberattack on Ukrainian government agencies in January prompted a statement by Ukraine's Ministry of Digital Transformation that "Moscow continues to wage a hybrid war and is actively building up its forces in the information and cyberspace"[4].

The Ministry's statement, which highlights the aim of the attack as having been to cause as much damage as possible to the infrastructure of state electronic resources, provides a new reminder that **where cyberattacks have served as a hallmark of hybrid threat activity, infrastructure is at the heart of hybrid warfare.**

Leveraging our global insights into state-level cyberattacks executed on and through mobile telecom infrastructure, this paper announces our identification of an advanced complex platform comprising a dynamic constellation of globally-dispersed mobile telecom nodes that we have designated the HiddenArt platform. To put the potential capabilities of such a threat platform into context, this paper presents a model whereby the weaponization of mobile network infrastructure might be utilised as a conventional force-multiplier in offensive military action. The effects achievable are apt to stagger defenders even if expected because of the unprecedented scale and scalability of effect potentially realisable through same.

The potential for the execution of targeted telecom Denial of Service (DoS) attacks to be integrated with Electronic Warfare (EW) measures against Ukraine presents an attack model consistent with reported Russian military doctrine describing modern warfare as entailing "the integrated utilization of military force and forces and resources of a non-military character"[5].

2.1 Hybrid Warfare

The term 'hybrid war' or 'hybrid warfare' refers to a situation in which a country combines overt military force with other means of power[6]. In broad terms, these are typically broken down into 4 major types: diplomatic, military, economic, and technological[7]. While the terms hybrid war/warfare and 'hybrid threat' tend to be used interchangeably, we may distinguish between them however by asserting that a hybrid threat is a complex threat involving elements across any combination of the four different dimensions.

Hybrid warfare involves the combination specifically of military and non-military means of power. It is strongly associated with the exploitation of vulnerabilities presented by the growing interconnectivity of systems globally. Accordingly, it naturally tends to be associated with cybersecurity threats and cyberwarfare, which might be considered elements of hybrid warfare. The defining element of hybrid warfare however remains the use of force[8].

For the better part of the 21st century, the concept of hybrid warfare has been subject to much debate. Despite the now widespread use of the term in defence and security circles, as well as in academic, policy, and journalistic discourse, the use of the concept continues to be criticised today as it was when first popularised by Frank Hoffman in 2007. While Hoffman's original model that blurred the boundaries between regular and irregular warfare drew widespread attention, his use of the term hybrid drew criticism from various quarters for its perceived ambiguity and lack of strategic validity.

Both then and still today however, the term has been most frequently dismissed by detractors with the assertion that it falsely ascribes newness to characteristics held to have been inherent to warfare throughout history. With regard to Russia in particular, it has been dismissed as a 'label'[9] of little analytical utility in explaining the Russian invasion of Ukraine in 2014, or Russian strategy or actions - let alone military doctrine, then or since[10].

Accordingly, academic discussion of hybrid threats particularly in the West has tended to run aground on the questions of the newness of hybridity in warfare, or of the hybrid-ness of Russian aggression. However, an increasing number of national competent authorities, security practitioners and policy makers, among others besides, have focused on questions of what 21st century multimodal warfare can do, how it may be evolving, and why it is critically important to defend against into the future.

The immediacy of these questions stems from a recognition - particularly in the context of European security - that the aggregated effects of the activities generally grouped under the term hybrid warfare comprise a range of coercive and subversive measures involving conventional and unconventional means (of power) which are consistently:

- synergistic in execution;
- cumulative in effect;
- strategic in implication;
- deliberate in purpose;
- damaging to open and democratic institutions, systems, and countries;

– and yet are characteristically ambiguous in manifestation.

As this implies, it is widely recognised that the effects of hybrid activities often prove conducive directly and indirectly to the interests and objectives of state-level actors antagonistic to the rules-based international order. Indeed, the European Commission describes the coordinated use by hybrid threat actors of a mixture of diplomatic, military, economic and technological measures to exploit vulnerabilities as "one of the most complex and constantly evolving challenges" faced by the European Union and its Member States[11].

However, the potential utility presented to state-level threat actors of mobile network based attacks for cyberwarfare and **the potential weaponization of telecommunications infrastructure in hybrid warfare has up to now not been sufficiently acknowledged.** Indeed, recognition of mobile network security even as belonging to the domain of cybersecurity is only just beginning. As the Fourth Industrial Revolution continues to accelerate, the increasing digitalisation of the services and functions we depend on will place ever-greater emphasis on the role and relevance of mobile telecoms for societal, economic, and state security.

The growing significance of telecoms services and infrastructure as a potential hybrid threat vector is illustrated in the chart below. Using categories set out in the recent report by the Hybrid Centre of Excellence: 'The landscape of hybrid threats: a conceptual model'[12], it might be shown that at least 7 of the 13 different domains identified are directly implicated by telecoms-enabled threats. The framework is adapted here to reflect the potential for the various strategic purposes of hostile actions executed at the less overt end of the spectrum of violence also to be supported by telecoms-enabled attacks. **This arguably makes mobile telecoms infrastructure a meta-vector for hybrid threats presented even where kinetic military action is not involved, as well as where hybrid warfare is waged outright.**

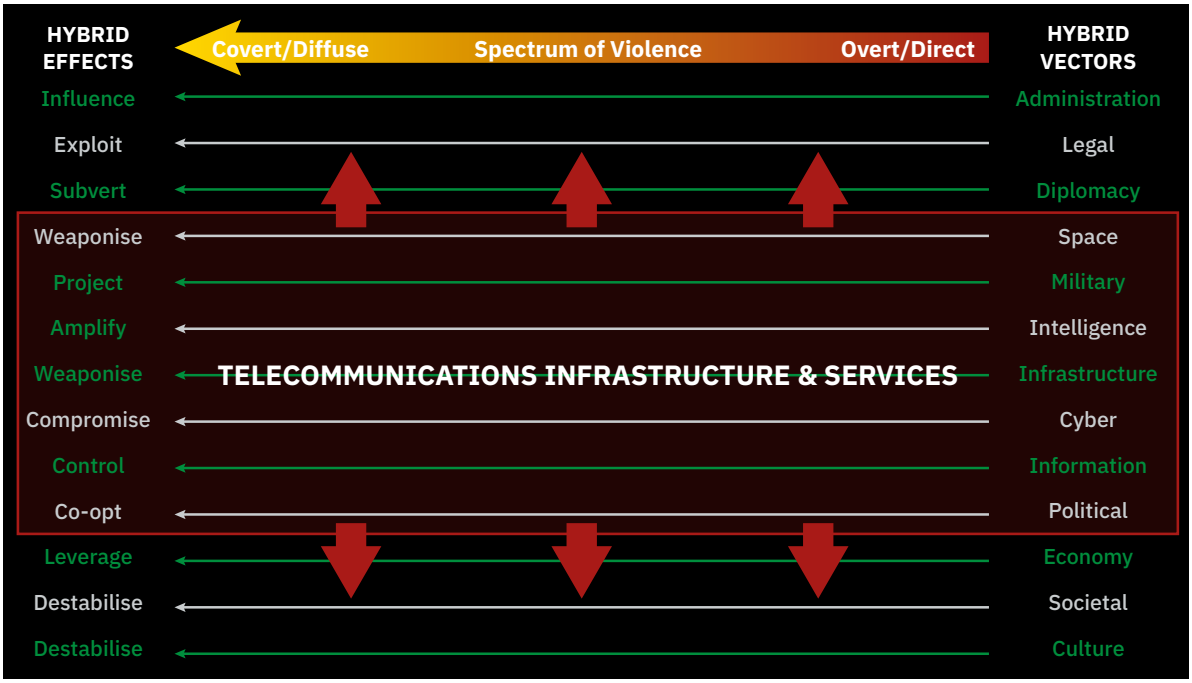


Figure 1: The growing relevance of Telecoms to Hybrid Threat vectors in Hybrid Warfare.

Such potential impacts achievable through mobile network-enabled attacks may be revealed across Europe and around the world in the event of a new invasion by Russia of Ukrainian territory. Without any doubt, a significant escalation of Russian kinetic action on Ukrainian territory will be seen by many to mark the next watershed moment in the evolution in hybrid warfare. The real inflection point however may be one of Russian willingness to risk exposing for the first time the full potential of a capability already long since possessed – that of conducting large scale attacks over mobile networks. It is here that any new offensive action may prove most surprising in the combination of military and non-military means of attack precisely where the technology involved - mobile network signalling – and the technological vulnerability exploited - is considered to be one of the oldest yet still most fundamental.

3 Mobile Network Attacks Today

Telecom networks today are an aggregate of technologies, frequencies and communication protocols used to transmit information from one point to other points around the globe. They have evolved over time, layering new technologies and protocols over older systems to give new functionality and use cases. The single most widely used communication system in the world today are Mobile Networks, whose underlying technology evolved from fixed line voice networks, specifically a technology called SS7 [13].

Since its inception as a signalling system in the 1970's, SS7 was designed to generate reliable and billable events for the setup and control of voice calls. A key concept of this network, for security reasons, was the separation of the user-plane (the voice calls, which the user has access to) and the control-plane (the signalling used to setup the voice call, which the user does not have access to). As mobile networks emerged and developed in the 1980's and 1990's, the SS7 protocol evolved to have new layers which allowed the setup and control of mobile devices. However, the separation of the user-plane and control-plane continued.

When deploying mobile networks, they are logically thought of as having two parts:

- The Core Network, and
- The Radio (Access) Network

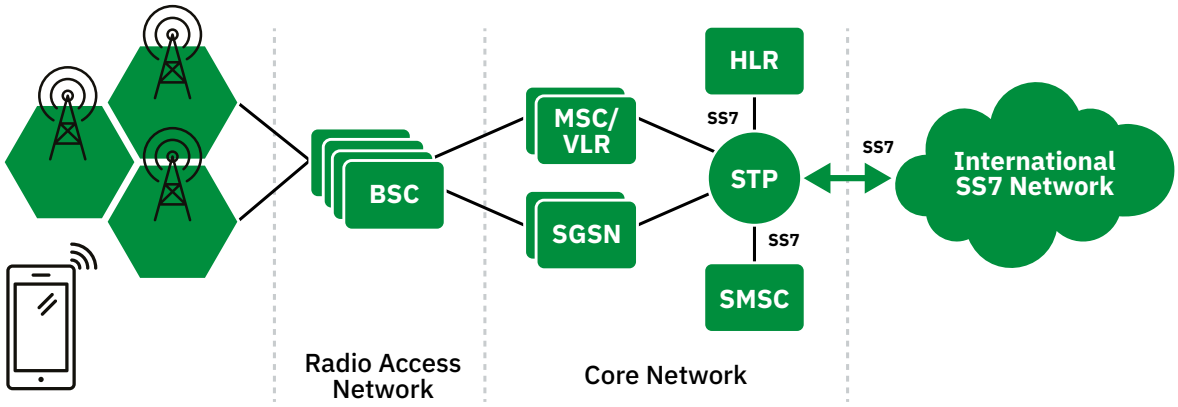


Figure 2: Simplified 2G/3G Mobile Network with SS7 Interconnection

The Core Network is where the brains of the mobile operator reside. It directs and marshals the user-plane traffic from the Radio Access Network, as well as being the interface to the rest of the world. It does this by generating control-plane SS7 commands - or packets - that are sent between the different core network nodes for the many subscriber events, as well as sending SS7 packets worldwide for events that involve subscribers from other Core Networks. A key concept of these Core Networks is that access to these control-plane links are very tightly controlled by the mobile network operators worldwide.

As networks evolved, and 3G, 4G and (now) 5G radio networks have been deployed, new core network protocols and technologies have also come into use, using Diameter(4G) and HTTP/2 (5G). However, unlike on the Radio side, these protocols rarely replace directly protocols used in the core network side, in fact in many cases they build on top of the presence of the existing protocols [14]. More importantly, the concept of a control plane and user-plane separation is the same for these, as well as the fact that access to the control-plane should not be given to unauthorised parties. This 'assumption of trust' model - that only those who should have access, will have access, was eventually proven to be fundamentally flawed in 2014.

In 2014 there were multiple revelations and news releases[15] concerning mobile core networks and privacy vulnerabilities. While the vulnerability of unauthorised access had been known for some time, in that year it was shown that there were threat actors (state-level actors and surveillance companies) that had access to the mobile core network. At the same time, Researchers also showed an even greater extent of attacks possible if they were to be given access[16].

Fast forward to today, and it has been definitively shown[17] that mobile core networks are a contested space and a constant target. Currently there are a range of threat actors identified active in this space, who all have differing aims:

- Organized Crime Groups (OCGs)
- Surveillance Companies
- State-level Actors

The types of attacks possible by these threat actors using core networks can vary, but at a high level the following are possible:

- Surveillance/location tracking
- Message/Call/Data Interception
- Fraud (against the operator or the subscriber)
- Phishing* (malware delivery)
- Denial of Service
- Information harvesting

**Note: Phishing via SMS. SMS is an unusual case as it is a 'user-plane' type communication from a device, but it is transported via control-plane protocol. As a result, it can be injected via mobile devices or via direct control-plane access*

In general, if they get full access, then OCGs for example are primarily interested in using access to this network for interception of text messages to compromise 2FA security for financial gain.

Surveillance companies and state-level actors are often closely aligned in their aims, which is natural because the end customers of surveillance companies are typically government entities. Observed behaviour of these two entities is primarily location tracking, and communication interception. Information harvesting is often required for all threat actors as a by-product to executing attacks successfully and to develop further attack potential over time.

Detecting malicious attacks requires mobile operators to have invested in defences. However, accurately attributing the real source and threat actor requires expertise and advanced intelligence. One difficulty in identifying and attributing these attacks is differing malicious attacks from noise. Assuming that every unusual activity is an attack, or attributing to country of origin is not sufficient (or normally correct), and doing so can lead to incorrect conclusions[18].

Once it is determined what is an attack, and what is not, one interesting aspect of the mobile network security space is that of the identified malicious attacks, criminality only accounts for a small portion of these. There are potentially many reasons for this, not least due to the cost in getting access, the expertise required to execute attacks, and the consequences of detection. In addition, other types of malicious activity seen in other cybersecurity spaces, such as low-skill (so-called 'script-kiddie') bulk attacks or hacktivism, are essentially on mobile signalling networks.

In general, the majority of threat actors on the mobile signalling network are characterised by being stealthy, innovative, and inevitably financed directly or indirectly by a state-level actor.

4 Potential use of Mobile Network Attacks in offensive military action

4.1 Mobile Network Attacks – warfighting relevance

Approaches to Electronic Warfare (EW) have significantly evolved over time, broadening in scope for operations in the greater electromagnetic spectrum beyond its traditional application in monitoring and disrupting military radio signals. While EW has accordingly come to encompass electronic attack against new types of targets presented in the modern information environment including mobile telecoms[19] - the full force-multiplying potential offered by the synergistic integration of mobile network-enabled attack into EW measures has yet to be widely acknowledged.

Even if it were the case however that this had never been observed, nor even yet been deployed on the battlefield, it is predicted by the classification of cyber capabilities as a form of EW weaponry[20] and the ongoing convergence of EW, cyberwarfare, and information warfare approaches[21].

Of course, wherever conventional asymmetry is assured for military forces, there would be no tactical or operational imperative to draw upon mobile network attack capabilities and risk exposing them needlessly (prompting efforts to defend against their future use). Wherever conventional asymmetry is not assured at the tactical and operational level however, force multiplication enabled by non-military means in this way can generate asymmetric advantage in military confrontation through network effects. As Russian Chief of the General Staff, Valery Gerasimov himself asserts: “No matter how perfect an opponent’s forces are, vulnerabilities will always be found”.

This section will focus on two possible use cases where access to mobile telecom networks could be used to attain and further amplify advantage in offensive military operations. Firstly, we will outline how Denial of Service (DoS) attacks via mobile networks could be used, in effect, as a military force multiplier by enhancing targeting of military forces. Even according to past criticism of the concept of hybrid warfare, the combining of military and non-military capability together in such a way - i.e. their integrated use – justifies qualification as hybrid warfighting. Secondly, we will outline some ways in which location tracking, call interception, and other attacks can be used to further a hybrid war effort by projecting mobile network attacks throughout targeted territory.

These use cases are, of course, not mutually exclusive. Indeed, they are highly compatible in execution and potentially mutually reinforcing in their aggregated effects. Other use cases are also possible, including combinations of the two presented here. In each use case, the mobile network-enabled attacks outlined offer clear potential to be leveraged in a way that is consistent with hybrid warfare. The following are two potential use-cases illustrating these principals.

Example Use-Case #1: Mobile Network-Enabled Denial of Service for Military Targeting.

The type of telecommunications-based attack that offers readily-realisable potential for use in this respect is a targeted DoS attack executable remotely via globally-vulnerable signalling protocols on targeted mobile networks. With certain conditions met, such an attack might be used as unconventional analogue and battlefield counterpart to the conventional EW technique of military communications jamming, among other capabilities. Beyond merely offering an extension of jamming capability, additional network effects are gainable where the psychological component of EW can be exploited in the coordinated use of both capabilities in combination within a single unified battlespace.

Wherever offensive forces can bring to bear both military EW systems and telecom-enabled attack capabilities, battlefield reconnaissance can potentially be augmented through the generation of real-time targeting information enhancing the military kill chain. **Force multiplication might therefore be described as attained through the generation of a hybrid kill chain (understood as the combined military and cyberwarfare kill chain effects).**

This may be achieved with sufficient integration of command and control systems with wider entities. It requires structures enabling coordination between the military and non-military entities able to access and manipulate the electromagnetic (EM) environment in selected areas where targeted units are located, and the creation of effects to influence their behaviour. Combined, these capabilities can be used to prompt the transmission of military and non-military communications by targeted units in a controlled way offering the potential, for example, to support triangulation of their positions and refine the attacker's intelligence picture of the real-time battlefield disposition of the targeted forces. This could also yield further cyber targeting potential besides however where new identifiers (for individual pieces of equipment/platforms) may be associated with specific targets thereby inducing further potential vulnerability through the psychological component of EW.

In contrast however to the well documented use of EW assets for psychological attacks that are overtly aimed at being harmful (to that end, deliberately disclosing the attacker's intent) – such as those reportedly involving the delivery of text messages directly to targeted soldiers' phones for example – the psychological effect in this DoS instance is much more subtle, and yet also much more likely to induce the intended behavioural response than any direct psychological attack. It relies on the fact that many members of even frontline military forces today might be expected to be carrying mobile devices including personal phones. It also relies on the reality that despite the introduction of rules aimed at controlling access by personnel to mobile services, compliance can be difficult to ensure, and mitigation is not always possible.

On the principle therefore that many military personnel today routinely have - and will seek to retain - connectivity for mobile network services in addition to military communications networks wherever possible, their behaviour may be influenced to create exploitable vulnerabilities consistent with the principles and purpose of hybrid warfare.

Where the requisite combined access to the EM spectrum in the battlespace is afforded to the attacker and connectivity to civilian mobile networks is sustained by targeted forces, the latter's military personnel might be expected to react to the execution either of:

- Denial of Service attacks on civilian mobile core network nodes, or
- the jamming of military comms by EW systems (in combination with other EW capabilities)

by reverting to the available alternate method of communications in a characteristic way in the moments immediately post-attack in either instance.

An SS7-based Denial of Service attack executed to disrupt targeted personnel's access to the civilian mobile network in a specific region might be expected to prompt observable and capturable bursts of military transmissions in response to the attack as units seek to report the event in an effort, as before, to maintain and maximise situational awareness within the battle space. In conjunction with the use of military radio frequency (RF) direction finding equipment, this could enable the identification of targeting selectors that may be associated with specific military units and potentially even correlated with individual members of same.

The converse sequence of deployment might similarly yield real-time targeting information. It could begin with offensive military units using EW systems to degrade defender military command and control communications in targeted areas at a specific time for the express purpose of prompting an observable, capturable, and exploitable response over civilian mobile networks. The assumption in play is that military personnel would attempt likely attempt to use mobile devices, however counterintuitively, to maintain situational awareness.

This can be expected to yield potentially exploitable information both in terms of communications that may be associated with devices already attached to mobile network nodes and the appearance of newly attaching devices switched on in response to the attack on military communications, however briefly. Other attacker-controlled capabilities such as IMSI-capturing platforms might also be potentially integrated to achieve similar hybrid synergies and force-multiplication in the subsequently enabled conventional attacks (such as artillery fire) on targeted positions.

Such an attack model is consistent with the concept of constructive 'reflexive control' (RC)[23], which deals with measures aimed at compelling an enemy to make decisions to the advantage of the attacker particularly where they can be anticipated to adhere to known doctrine. Since the behavioural response prompted by RC in this instance would likely constitute a violation of military doctrine on the part of successfully-targeted forces (e.g. prompting their use of personal mobile devices after a military comms disruption), this might also be considered a form of destructive RC and a hybrid threat.

A larger-scale coordinated execution of mobile network DoS attacks offers a means for an attacker to project force throughout targeted territory through simultaneous telecoms-enabled attacks on civilian centres of power, in addition to military formations, to disrupt decision-making and degrade strategic response.

Example Use-Case #2: Mobile Network-Enabled Targeting for Surveillance & Intelligence purposes.

Mobile network-enabled attacks may also further other warfighting objectives identified in military theory, such as the execution of simultaneous effects throughout the entire depth of enemy territory, as included in Gerasimov's 2013 article: *'The value of science in foresight: new challenges demand rethinking the forms and methods of carrying out combat operations'*[24]. The emphasis placed on 'the achievement of political goals' as the purpose driving 'change in the character' of warfare in a chart included in Gerasimov's article (shown in translation below) is noteworthy.

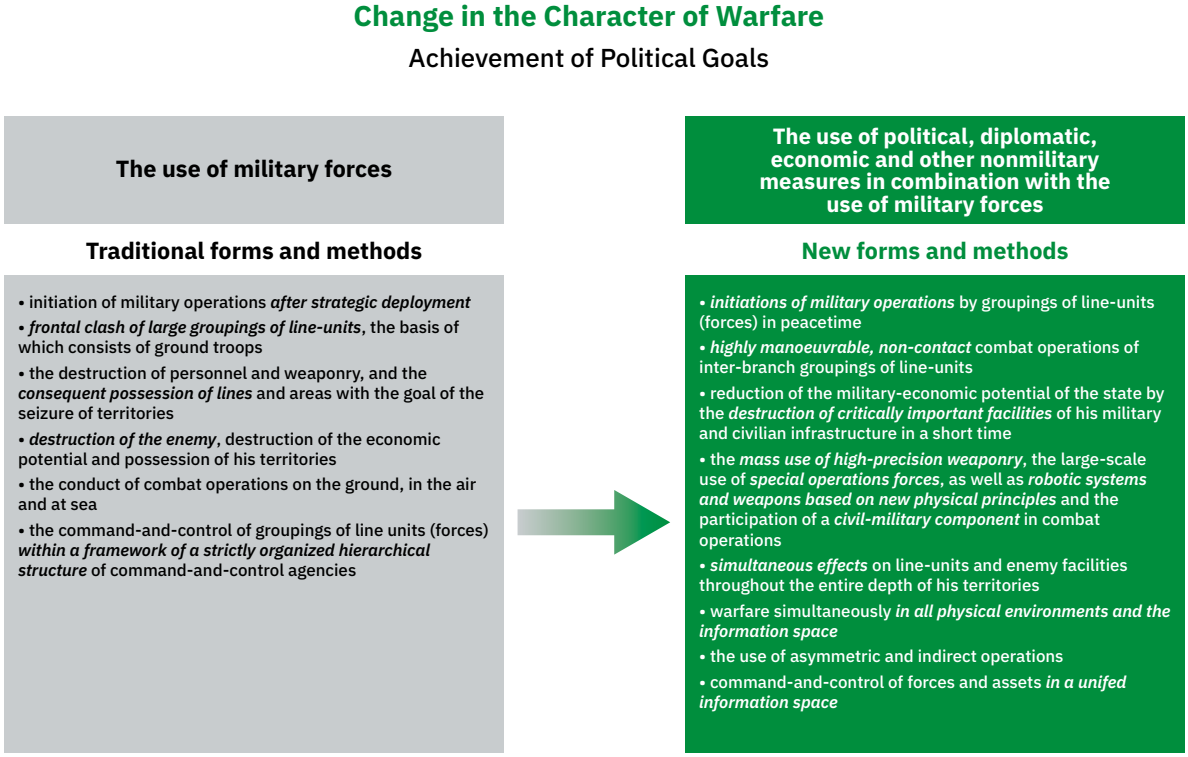


Figure 3 : Change in the Character of Warfare[43].

To embellish Clausewitz's famous dictum: if 'war is the continuation of politics by other means', hybrid war is the extension of warfare by non-military means.

The types of mobile telecom network attacks that might be executed to extend effects throughout the entire depth of an attacked territory include - but are not limited to - signaling-enabled location tracking of targeted individuals, and the interception of communications. The targets in such instances tend to be comparatively small in number but of very high importance in their respective spheres, such as political, military, or industry-related activity. In this respect, mobile telecom network-focused attacks of this kind exhibit the same overall characteristics as the most significant state-level cyberattacks associated with the targeting of I.T. networks in that they appear comparatively low in incidence but are typically high in potential impact.

Leveraging the AdaptiveMobile Security's Signalling Intelligence Layer (SIGIL)[25] solution for global insights into organised cyberattacks executed on mobile network infrastructure, it is assessed that 'HiddenArt' actively sustains a capacity to remotely access the personal devices of targeted individuals around the world on an ongoing basis. These kinds of attacks, whether executed over SS7 (2G/3G), Diameter (4G), or other protocols, also exhibit other characteristics commonly associated with prominent state-level cyberattacks. These include, for example:

- the ability to hide attacks (and their 'presence' within national mobile network infrastructure);
- an ability to compromise a network and move laterally within it;
- an ability to adapt attacks in individual instances to sustain ongoing targeting;
- reconnaissance of networks on an ongoing basis (sometimes called 'probing' attacks);
- data exfiltration (such as for: for identifiers and information 'harvesting');
- an evolving attack methodology able to exploit the ongoing evolution of mobile telecom networks;
- an overall upward trend in sophistication, ambiguity, and potential costs implicated;

Such attacks, when executed by an actor with capability, persistence, and aggression, have the potential to pose a national security threat to any country whose citizens may be targetable over mobile network attacks. The threat can rise to this high level where a number of factors are present, including:

- where such targeting is achievable over an extended period of time – primarily enabled by the comparative difficulty for authorities in such states to gain access to reliable and timely intelligence;
- where the individuals targeted may be identified as stakeholders in matters of strategic interest, whether in a national context (of a targeted individual's own country's interests), a domestic context (of the state-level threat actor's interests), or an international context;
- where the potential scalability of such attacks is not well understood by those individuals who may be likely, for various reasons, to present a target to a state-level actor.

There are three main drivers of the scalability of such attacks. In the first place, the evolution of attack methods due to the advance of technology has introduced the potential for the migration of device compromise to wider network compromise. This migration is not always vertically to the more advanced technology, but could move laterally or even downward to technologies no longer protected or even considered in the more advanced ecosystem.

An attack method of unprecedented sophistication, called Simjacker[26] discovered by AdaptiveMobile in 2019, showed the potential for mobile threat actors to load malicious commands via SMS onto the SIM Card on the targeted individual's device. This location tracking method was used by a threat actor in order to bypass mobile network protection in place on the more advanced network interfaces. The potential threat associated with orphaned vectors will trend upwards as the mobile network threat continues to mature.

Another way mobile telecom attacks may be scaled is by separate, further exploitation subsequently of data exfiltrated from compromised devices (defined as any device that has been successfully associated with an identified individual, and which has been shown to be 'reachable' – i.e. is vulnerable to attack – via mobile network protocols). Beyond the additional targeting potential offered to threat actors like HiddenArt by such data, it may be shared with partner state-level cyber threat actors as selectors exploitable for their own cyberattacks as part of a wider cyberwarfare campaign against the same target(s) and the institutional networks accessible on targeted devices.

A third way that targeting can be scaled is through the operations of networks of human actors deployed into the countries of targeted individuals. Human Intelligence (HUMINT) operations conducted by such actors – the officers, operatives, and agents of Intelligence and Security Services – can serve as a human 'force multiplier' for mobile network threat actors by acquiring targeting information through their own network access. In the context of hybrid warfare, a relationship between such Services and a threat actor like HiddenArt could possibly comprise a common set of actors "behind the hybrid threat" who are able "to use their intelligence services [with the] capability to conduct clandestine operations and their sometimes vast networks"[27] After all, *"to the extent that intelligence can support and has been used to support a wide range of hybrid threat activities, it can be understood to be related to all other domains"*[27].

Rationale for a Mobile Network Attack Capability

It is important to note that the acquisition of such a capability to execute and scale mobile network attacks – which is built up by the execution itself of numerous attacks over time as outlined above - is not sought after the onset of offensive military operations. Rather, its development is pursued long in advance and in preparation for precisely that contingency. So where in the past, Soviet military doctrine held that war is not declared but begun with an *"already developed military force"*[22], any new invasion of Ukraine could be begun with already developed military forces enhanced by combined operations involving weaponized civilian mobile network infrastructure.

A potential indicator of development towards such a combined approach to warfare is the reported creation in Russia of a cross-government framework aimed at the integration of military and non-military capabilities held by entities including the Ministry of Telecom and Mass Communications[28].

Overall, there are a number of added benefits in leveraging the capability to attack mobile networks in this way. In the first place, the network infrastructure supporting such mobile attacks via signaling protocols is globally-dispersed. This provides significant redundancy to adapt and sustain attacks in the event that any of the malicious signaling sent is successfully blocked at any point. The international reach of mobile network threat actor, like HiddenArt, also allows a degree of deniability due to the difficulty in detecting the true attack traffic amid the immense volume of non-malicious traffic that is generated daily by mobile networks the world over.

Deniability might also be achieved through the use of a company offering offensive mobile network (and other cyberwarfare) capabilities for purchase or as a service. The rise of such companies represents a new driver of instability and uncertainty in the international security environment as it makes it increasingly possible for state-level actors to use such companies effectively as proxy actors for themselves in attacks executed globally. Another potential added benefit for an attacker is that the ability to achieve force multiplication through combining mobile telecom network-enabled attack with military force can alleviate the imperative for continued procurement and defence spending requirements to maintain the trajectory of EW capability development.

Given all of the above, the threat presented by a military aggressor could be amplified by the force-multiplying potential of mobile telecom-enabled attacks.

4.2 Applicability of the Threat

Previously we discussed the potential uses of mobile network attacks in combination with military measures consistent with accepted principles of hybrid warfare. Based on the maxim that Vulnerability x Threat = Risk, then in order to determine the true Risk attached to a Vulnerability, we need to establish if there is a capable and present Threat that can utilise the vulnerability in mobile networks. The following are the reasons why we judge that there is a present threat:

Previous History of usage: Ukraine Surveillance, Call Interception & DoS Incidents (2014)

As outlined in our blog on this incident[29], the world's first reported incident of mobile core network attacks (or external interference) was reported in May 2014. At this time, a report was issued by the Ukrainian Telecom Regulator (NKRZI). This document[30] - which went unreported by the press outside of Ukraine & Russia - contains the result of the investigation of the NKRZI, assisted by the Ukrainian Security Service (SBU), into SS7 activity over several days in MTS Ukraine. The results of this report were that over a 3-day period in April 2014, Ukrainian mobile subscribers received suspicious/custom SS7 packets from multiple SS7 network elements allocated to Russia, causing their location and potentially the contents of their phone calls to be obtained.

Although no targets were named, as we reported around this time, there were several sensitive phone calls that were reported to be intercepted and their contents uploaded to the internet. The common thing about these is that they involved senior political individuals[31] discussing sensitive topics, either in Kyiv far from the border or in other countries[32]. This makes the possibility that these calls were intercepted by fake base stations very unlikely, and that SS7 techniques were more likely to be used - successfully in this case. Given the documented records of SS7 attacks and incidents of calls being intercepted we can safely say there is precedent in this field. In addition, as this took place nearly 8 years ago, we can assume that this capability has been retained and expanded since.

An additional previously reported mobile network-targeted attack was the Denial of Service attacks on the mobile phones of members of the Ukrainian parliament at the height of the Crimean conflict in 2014[33]. At the time these was reported to be IP telephony attacks, enabled by equipment installed in the networks of Ukrtelecom in Crimea. These attacks, properly termed Telephony Denial of Service (TDoS) attacks - if generated by IP telephony - would have originated on fixed line networks, but would have actually terminated on Ukrainian mobile networks through voice interconnects. Strictly speaking, these attacks could have been executed without needing insider Ukrtelecom network access, but if insider access was used then that would make attacks more direct and harder to stop. In addition, in order for the attack to succeed, all of the phone numbers of the targeted MPs and other individuals would have needed to be known in advance.

Improving Offensive Intelligence: ENFER (2021)

In March 2021, the Atlantic Council issued a report[34] on 3 entities engaged in cyber proliferation: NSO Group, DarkMatter and a Russian entity codenamed ENFER[35]. ENFER is classified as *"assisting the Russian intelligence services with its offensive cyber operations, building up capabilities that Russia may decide to use against strategic adversaries."* What marked out ENFER as being unique to the other two well-known entities is its research and development within the mobile network space. Specifically: *"significant and unique capabilities were provided that focused on Signaling System 7 (SS7) telecommunications networks."*

According to this report ENFER would reportedly use vulnerabilities identified in assessments of telecom operators to be *"... exploited for operational objectives associated with ongoing espionage"*. This information obtained in a sanctioned vulnerability assessment is quite valuable, because in this period network and node information may be retrieved while the mobile operator is in a somewhat 'artificial' environment of permitting a wide variety of attacks to be executed. While every mobile operator is different, network nodes, including those involved in security, are from a finite number of vendors, and a flaw in one in one network is likely to replicated in other networks. Any information obtained in these tests by ENFER, and passed on to an offensive partner could then be re-used for future attacks elsewhere. While ENFER's name was not revealed by the Atlantic Council, media reports at the time[36] suggest that ENFER was one and the same as a Moscow-based Cybersecurity company sanctioned by the U.S. Department of the Treasury[37], one month after the Atlantic Council report.

Awareness of Dangers: RuNet Signalling Network tests (2019)

In November 2019, the Russian 'sovereign internet law', or RuNet initiative which came into law. Subsequently, in December 2019[38], Russia executed its first tests of this law. However, rather than internet based, these tests were mobile signalling (SS7 and Diameter) control plane tests and were done to understand and improve the defences of the Russian Mobile Networks.

Before these tests, the RuNet system had been understood by almost all observers[39, 40, 41] to primarily, or only, concern the internet within the Russian Federation. The fact that the external security of Russian mobile networks was also in scope in this law and system, and that the first tests for the entire RuNet system were on these links, shows the importance that the Russian authorities attributed to protecting these communication links.

These tests themselves with 18 different attack scenarios over SS7 and Diameter, with mixed results[42] - results which were no doubt have prompted the mobile operators to improve. To date Russia is the only country in the world to have reported publicly on the results of signalling security tests of their mobile network providers. This suggests a well-developed awareness of the offensive applicability of these protocols, which provides a rationale to ensure that defensive abilities would be in place.

AdaptiveMobile detected Russian-Associated Signalling Attacks: HiddenArt (2016->)

Since 2016, AdaptiveMobile has been tracking a signalling threat actor/platform which our intelligence has attributed to likely have Russian direction and control. This attribution is based on its behaviour, targets, and other intelligence. We have assigned the external designation HiddenArt to this threat actor.

The behaviour of this threat actor has varied over time. Initial attacks from HiddenArt primarily involved voice and text message interception of specific individuals over the SS7 interface, as well as location tracking. Targets of this group have included Russian political dissidents living abroad, as well as foreign (VIP) individuals. An example sequence of specific attack behaviour over a multi-day period is below.

In the below case multiple attempted reprogramming of several targeted subscribers' network settings, in order to effect voice call and SMS interception was performed via a SS7 command called ISD. There were also a large 'spike' of location tracking/ reconnaissance attempts in the middle of the period using a command called PSI, followed by an elevated level of further ISD call interception commands. Occasionally, a response command to the attacker node would be generated by the target network in the case of the targeted subscriber making a phone call (IDP) or SMS (IDP-SMS) of interest to the attacker.

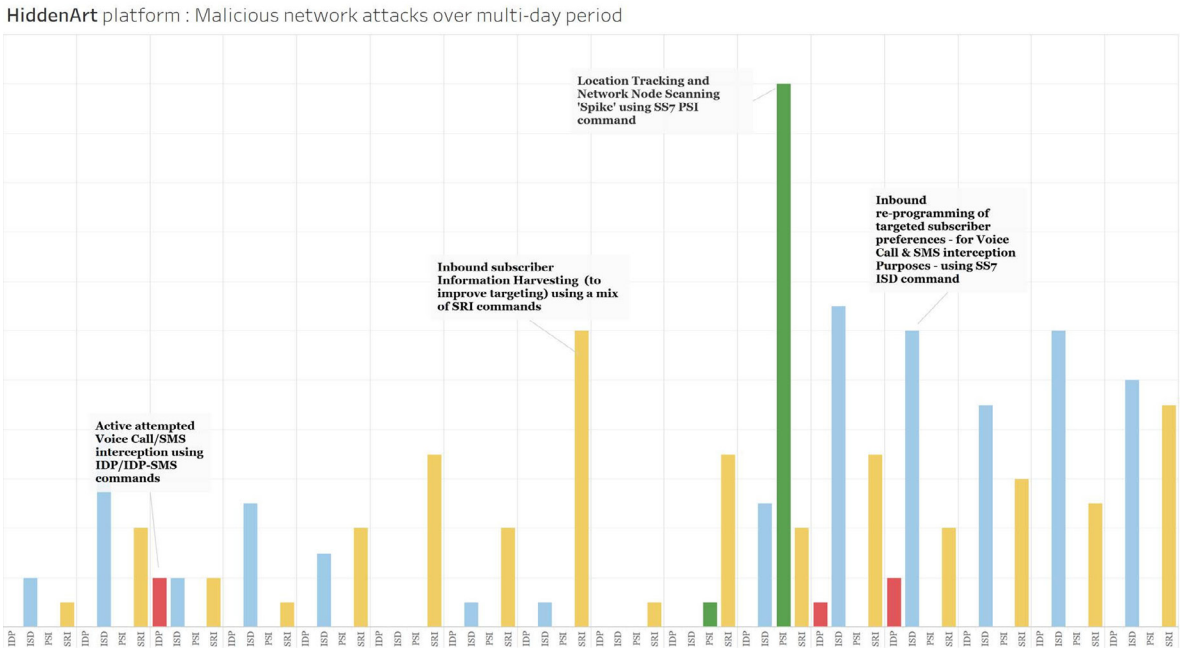


Figure 4 : Attempted Location tracking and Call & SMS Interception by HiddenArt group against target operator

These initial attacks purported to come (essentially 'camouflaged' or hidden) via an operator group in Africa who were unaware of the activity, but since then worldwide sources have been used. A unique defining feature of this threat actor, and the origin of part of its name, is that SS7 signalling source addresses used by HiddenArt are selected in order to 'hide' within similar but legitimate SS7 signalling source addresses.

Since detecting this threat actor we have observed it execute periodic reconnaissance activities in at least 7 target mobile networks around the world. However, given the wide geographic distribution of these targeted mobile operators, we assess the threat actor's activity is at a global scale. These attacks attempt to gather information on specific individuals while at the same time checking the security of the targeted mobile network. We have recently (Q4 2021) observed an uptick of reconnaissance activity globally from this threat platform. This ongoing reconnaissance and global scope indicate that this group has an extensive capability to execute a wide variety of mobile network attacks if needed.

Further specific details – tactics, techniques, and history - of this threat actor/platform are available within the AdaptiveMobile SIGIL (Signalling Intelligence Layer) system[25].

5 Recommendations to Protect

There are several general recommendations and specific recommendations we can make as an outcome of this paper.

First of all, malicious mobile network signalling attacks must be recognised as a state-level cyber threat to individual nations as well as to collective security, and an integral component of hybrid warfare. While all computer networks are valuable and important, mobile networks form part of the Critical National Infrastructure of a state, and an attack on them should be recognised accordingly. Actors like HiddenArt must be recognised accordingly as Advanced Persistent Threats (APTs).

At the same time, mobile operators alone should not be wholly responsible for organising, evaluating, and ensuring that adequate defences are put in place. State-level attacks will involve all mobile operators in a country, not just one, but a lack of visibility or immediate sharing of detected attacks will greatly compromise the state's ability to know and react to attacks. Also, these attackers have resources and skills which each mobile operator in the country may not have the ability to detect and counter. As a result, there will need to be intelligence and operational security sharing and direction at a state-level.

To start implementing defences, mobile networks in a country should implement the GSMA signalling security recommendations FS.11 for SS7, FS.19 for Diameter, and FS.20 for GTP-C. This is a starting point for mobile network signalling defences, however it is only a starting point and should not be relied upon as well-resourced attackers will find a way around any static defence, as shown in the Simjacker[26] attacks.

Also, in general, mobile operators in a country should analyse, either internally or externally, all detected unusual signalling behaviour. This should be done to understand the attacker's attempts to bypass defences and predict their future movements. Due to the volumes of unusual events (potentially several tens of thousands per day in a typical large network) that could be mistaken for malicious events, this will require advanced analysis by threat intelligence experts, combined with confirmed threat information from other sources. One way for mobile operators to do this effectively is via a managed network threat intelligence service. Machine learning, while useful to find initial suspicious activity, is of little value in interpreting what is truly malicious or not in these complex networks.

More specifically, all mobile operators in a country should put in place plans to handle attack scenarios which have not been encountered to date. As mentioned, hacktivist behaviour, and DoS attacks are essentially unknown in mobile signalling networks. The only known recent DoS attack occurred in Norway[43] where a million and a half mobile subscribers were knocked offline by mistake due to an unsanctioned SS7 penetration test. This lack of reported DoS attacks in the past may give mobile operators a false sense of security in assuming that locally targeted or large-scale DoS attacks may never happen, as they have not happened in the past. Mobile operators in a country should have co-ordinated, concrete plans in place to handle a variety of large-scale mass DoS, tracking or interception attack scenarios:

- These plans and solutions should be joined up and co-ordinated between all the mobile operators in a country because ingress routes to one operator in a country may be used to target other operators in a country.
- Next, these plans and solutions should be developed for a range of scenarios prior to any attacks. While adjustment during any ongoing attacks is expected, mobile operators should have a range of offensive scenarios – and their capability to defend against them - understood beforehand. Defensive examples could include the prevention of all roaming updates from hostile mobile network sources or links, or the implementation of more stringent roaming checks for specific subscribers who may be more likely to be targeted in an attack. These measures will be a trade-off as they will inevitably cause more false-positives, but will also provide a higher level of security which may be accepted by operators and the country during critical periods.

- Finally, tests or other inspection should be performed to prove these defensive scenarios are handled, or the level of shortfall known. It is better that limitations are understood and mitigated (or accepted), than assume security is present when it is not. Discovering that a signalling firewall cannot perform a specific defence during the middle of an intensive attack is not a risk any mobile operator should take with its subscribers. These tests should come from adequately vetted 3rd parties, and not be directly provided by the same entities providing the security nodes.

Again, the above ideally should be lead or co-ordinated at a state level, given the need to share information about attacks and to ensure defences are in place with no weak links. It must also be remembered that it is virtually impossible to know all potential signalling attack vectors that a resourceful attacker could deploy in a hybrid warfare situation. New types of attacks that were unforeseen are highly likely to be used. As a result, any signalling security system should be flexible, and new protection such as rules or call-flows should be capable of being put in place in real-time, rather than relying on code development or patches. Speed in implementing these may make the difference in any attack. Costs in both implementing this security and making any changes if required could be lessened by the selection of flexible, managed signalling security systems.

Summary

Currently, Europe is braced for a possible new invasion of Ukraine by Russia. This conflict is likely to feature a range of innovative warfighting tactics - both on the conventional and cyber battlefield.

A key, but under-appreciated aspect of this cyber warfare battleground is likely to be attacks over mobile telecom networks. This is because attacks in this area fall squarely into the sphere of hybrid warfare tactics. Telecommunications networks, and especially mobile networks, comprise a unique and critical element of the national infrastructure, but like many other communication systems, they also suffer cyberattacks from determined threat actors, including state-level actors. A notable difference in mobile network attacks is that in circumstance to date, threat actors on these networks have a vested interest in not jeopardising the operations of a network in order to perform targeted surveillance and interception, however these interests may no longer be aligned in the event of a conflict.

We theorize that mobile network attacks could be aimed at targeting military units or other entities, in order to enhance an attacker's conventional military force at the time. These attacks could be executed in conjunction with with conventional EW measures, but the difference is the the difference is that the mobile network attack range would be greater - i.e. further 'over the horizon' - while the impacts could be more focused yet also deniable (covert), especially in comparison, for example, to launching EW drone operations. Similarly, mobile network-based attacks could be launched at civilian (or other) decision makers and centres of power in the country (or globally) in order to delay, intercept and distort decisions or information needed for governmental control in the event of a conflict, as well as other reconnaissance reasons.

We also expect this possibility due to the evidence of similar, but smaller-scale historic attacks attributed to Russian sources in the past, as well as external assistance given to improve offensive operations and capabilities since then. This is further reinforced by the continued activity we have detected worldwide from the HiddenArt Advanced Persistent Threat platform.

Given this clear danger, concerned states must proceed on the basis that the capability and resources to attempt to execute large-scale attacks on mobile networks within their country is in existence. As a result, they need to plan how they could address and defeat the danger, both now and in the future.

It is not enough to assume that since a widescale destructive or reconnaissance attack has never occurred over mobile telecom networks, that it will never occur. While this paper has focused on the military applicability of a mobile network enabled attack and illustrated it with use cases in the context of a possible new Russian military offensive against Ukraine, the same recommendations can be applied to any state looking to insulate, prepare and protect itself from any possible similar attacks on their national critical communications infrastructure.

References

[1] https://www.hybridcoe.fi/news/on-going-hybrid-threats-against-the-eu-and-nato/

[2] https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/

[3] https://www.axios.com/ukraine-russia-cyberattack-hybrid-war-ef466666-3bcf-48ba-a32f-72c070b34b4a.html

[4] Kofman and Rojansky (2015) A closer look at Russia's "Hybrid War".

[5] https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

[6] https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en

[7] Hybrid Centre of Excellence(2021): The landscape of Hybrid Threats: A conceptual model – public version.

[8] Kofman and Rojansky (2015) A closer look at Russia's "Hybrid War".

[9] Renz and Smith (2016) After Hybrid Warfare – what next? Understanding and responding to contemporary Russia

[10] https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en

[11] Hybrid Centre of Excellence (2021) 'The landscape of hybrid threats: a conceptual model – public version'

[12] https://www.adaptivemobile.com/downloads/shielding-the-core

[13] https://info.adaptivemobile.com/securing-the-path-from-4g-to-5g

[14] https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-goaround-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

[15] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyonelisten-to-your-cell-calls-and-read-your-texts

[16] https://blog.adaptivemobile.com/how-surveillance-companies-track-you-using-mobile-networks

[17] https://www.theguardian.com/us-news/2020/dec/15/revealed-china-suspected-of-spying-on-americans-via-caribbean-phonenetworks

[18] Kjellen (2018) Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces

[19] https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

[20] Kjellen (2018) Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces

[21] https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

[22] Gerasimov (2013) 'The value of science in foresight: new challenges demand rethinking the forms and methods of carrying out combat operations'

[23] Vasara (2020) Theory of Reflexive Control - Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy

[24] Gerasimov (2013) 'The value of science in foresight: new challenges demand rethinking the forms and methods of carrying out combat operations'

[25] https://www.adaptivemobile.com/products/sigil-signalling-intelligence-layer

[26] https://www.simjacker.com

[27] Hybrid Centre of Excellence (2021) 'The landscape of hybrid threats: a conceptual model – public version'

[28] Minkomsvyaz,(Lobov et al. 2014; Petrovskii & Kravtsov 2016; Lobov et al. 2017, cited in in Kjellen (2018) Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces)

[29] https://blog.adaptivemobile.com/russia-ukraine-telecom-monitoring

[30] https://web.archive.org/web/20140704121302/https://delo.ua/get_file/id/nkrzimtsakt.docx

[31] https://www.bbc.com/news/world-europe-26079957

[32] https://www.theregister.com/2014/03/04/ukraine_cyber_conflict/

[33] https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-aservice/

[34] https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-aservice/#ENFER

[35] https://zetter.substack.com/p/sanctioned-firm-accused-of-helping

[36] https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking

[37] https://www.forbes.com/sites/emmawoollacott/2019/12/24/russia-cuts-off-its-internet-with-mixed-results

[38] https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

[39] https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

[40] https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-andimplications-for-russian-cyber-behavior

[41] https://www.bbc.com/news/technology-50902496

[42] https://blog.adaptivemobile.com/ss7-security-putting-pieces-together

[43] https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

About AdaptiveMobile Security

AdaptiveMobile Security, an Enea company is a world leader in mobile network security, everyday protecting over 80 Mobile Operators and billions of mobile subscribers and devices globally from fraudsters, criminals and nation states. We have the strongest 5G core network security team, who are designing, planning and building the very best in 5G core network security solutions focussing on threat-intelligence, security heritage and protocol correlation.

AdaptiveMobile Security brings a unique security perspective on real-time mobile network traffic. The global insight provided by our 5G, Signalling and Messaging thought leaders, security specialist teams and Threat Intelligence Unit, combined with our signalling and network protection software that sits at the heart of the network, ensures AdaptiveMobile Security remains at the forefront of the latest advancements in mobile networks and their security, and continues to be the trusted partner of many of the world's largest Mobile Operators.

For more information on how AdaptiveMobile Security can help you protect critical national communications infastructure from malicious mobile network attacks by state-level threat actors please contact **sales@adaptivemobile.com**

Legal Notices

Head Office

Ferry House, 48-52 Lower Mount St, Dublin 2.

Contact: sales@adaptivemobile.com

www.adaptivemobile.com

Regional Sales Contact Numbers

US, Canada, Latin America Sales: +1 972 377 0014

UK Sales: +44 207 049 0421

Middle East Sales: +97144 33 75 83

Africa Sales: +27 87 5502315

Asia Sales: +65 31 58 12 83

European Sales: +353 1 524 9000

Regional Operational Support Contact Numbers

UK: +44 208 584 0041

Ireland: +353 1 514 3945

India: 000-800-100-7129

US, Canada: +1 877 267 0444

LATAM: +525584211344