FRAZER-NASH CONSULTANCY
A KBR COMPANY

Securing Space Based Solar Power as Critical National Infrastructure

Issue 1, May 2025

fnc.co.uk

Abstract

Space Based Solar Power (SBSP) has the potential to deliver consistently reliable power to a nation's electrical grid or energy intensive process 24 hours a day 7 days a week, making it critical to a nation's infrastructure.

It will be capable of generating significant revenue for its owner and will likely disrupt the current energy market.

Additionally, it represents a new technology potentially utilising transmission mediums that have been historically misunderstood and misrepresented in society. Each of these attributes has the potential to expose SBSP systems and operators to threats seeking to disrupt the development of the technology, attack a nation's energy supplies, extort money from the operator, or prevent the construction of a facility, additionally non-hostile threats may also impact SBSP. This paper seeks to identify and analyse the potential security threats posed to a SBSP system, how they may translate into risks for a typical SBSP system and discuss possible risk mitigations.

The paper considers the geopolitical and social implications of an SBSP system, including the associated astropolitics, international energy security, and potential societal reaction. In addition, the paper undertakes a high consequence event review for a generic SBSP architecture, identifying typical critical systems, likely threats and high-level mitigations.

Audience

This paper is intended for organisations that are developing commercial SBSP capability at a scale where it could potentially be considered critical national infrastructure. Its purpose is to progress the conversation about security for SBSP and help inform risk assessments and support the development of secure and resilient SBSP systems.

In this paper we have focused on the unique security challenges of SBSP and tried to avoid the security challenges that are shared with other existing energy and space infrastructure. e.g. the perimeter security of a power station or launch vehicle security.

Executive Summary

Space Based Solar Power (SBSP) represents a transformative technology with the potential to provide continuous, reliable power to national grids, significantly impacting energy markets and infrastructure. This paper explores the strategic and security implications of SBSP, focusing on potential threats, geopolitical considerations, and risk mitigation strategies.

Key findings

1. **Attractive target for adversaries:** SBSP systems, like other critical energy infrastructures, are likely to be targeted by well-funded and organised adversaries throughout their lifecycle.
2. **Public perception:** The adoption and security of SBSP technology will heavily depend on public perception, particularly regarding the safety of power beaming.
3. **Evolving threat landscape:** The threat to SBSP systems will increase over time as adversaries' tools and tactics evolve. However, resilience will also improve with advancements in counter-threat technologies.
4. **Comprehensive security approach:** Security measures for SBSP must address supply chain, ground, network, and in-space threats through a system-of-systems approach.
5. **International collaboration:** Collaborative international agreements can help mitigate risks and unlock the potential of SBSP. Strategic sharing of power sources may also enhance security against state actors.
6. **Adoption of security standards:** Early adoption of security standards like IEC 62443 and Cyber Informed Engineering (CIE) will be crucial for developing secure SBSP systems.
7. **Insider threats:** Mitigating insider threats through a strong security culture and limiting insider vulnerabilities is essential.
8. **Physical and structural resilience:** The physical location and structure of SBSP systems in orbit limit potential threats compared to terrestrial energy infrastructure.
9. **Debris generation deterrent:** The risk of space debris generation (Kessler syndrome) will for some aggressors act as a deterrent against kinetic attacks on SBSP platforms.

Find out more

You can learn a bit more about the authors and how to get in touch with us on the back page.

Geopolitical and societal cconsiderations

- **Astropolitics and energy security:** SBSP systems will influence strategic and political issues in space, impacting international energy security and astropolitics.
- **Public engagement:** Proactive engagement and transparent communication are necessary to address public concerns and build support for SBSP.
- **Regulatory frameworks:** Compliance with international and national regulatory frameworks is essential for the secure operation of SBSP systems.
- **Neocolonialism:** How power is shared between states will need to be carefully considered.

Security threats and mitigations

- **Threat actors:** Nation states, organised criminals, hacktivists, activists, and insiders pose various threats to SBSP systems.
- **Ground station security:** Key vulnerabilities include loss of safety systems, spacecraft control, and critical equipment theft. Mitigations involve robust security measures and regulatory compliance.
- **In-orbit systems:** Threats include unauthorised remote access, control hijack, and physical attacks. Mitigations focus on engineering-grade protections and defensive systems.
- **Future threats:** Advancements in AI, quantum computing, and counterspace capabilities will shape the future threat landscape. Continuous monitoring and adaptation are necessary.

Key recommendations

1. **Adopt Cyber Informed Engineering (CIE):** Integrate CIE principles into the design, build, and operation of SBSP systems.
2. **International standards:** Use internationally recognised standards like IEC 62443 for cybersecurity.
3. **Risk assessment:** Conduct comprehensive risk assessments and integrate appropriate mitigations.
4. **Regulatory engagement:** Engage with regulators early and comply with frameworks like NCSC's CAF or NIST CSF.
5. **International collaboration:** Build multinational partnerships and agreements to share energy and enhance security.
6. **Public engagement:** Learn from past infrastructure projects to minimise activist harm and build public support.
7. **Supply chain security:** Ensure supply chains demonstrate robust cybersecurity arrangements.
8. **Post-quantum encryption:** Plan for the transition to post-quantum cryptography.
9. **Insider threat management:** Foster a security culture that reduces insider vulnerabilities.
10. **Continuous threat monitoring:** Maintain awareness of the evolving threat landscape.

Conclusion

SBSP systems offer significant strategic and economic benefits but also face unique security challenges. By adopting a comprehensive security approach, engaging in international collaboration, and fostering public support, the potential of SBSP can be realised while mitigating associated risks.

Introduction

The concept of Space Based Solar Power (SBSP) has gained prominence in recent years, with several countries investing in research and demonstration missions, including the UK, US and China.

With falling launch costs and advancements in technologies for areas such as in-orbit assembly and wireless power transmission, SBSP is now considered to be feasible. A 2021 report by Frazer-Nash Consultancy, commissioned by the UK Department for Business, Energy and Industrial Strategy (BEIS), undertook a techno-economic assessment of SBSP, concluding that:

- SBSP is technically feasible, and could support Net Zero pathways.
- It is affordable, with a competitive Levelised Cost of Electricity.
- Development of this technology would bring substantial economic benefits for the UK [30].

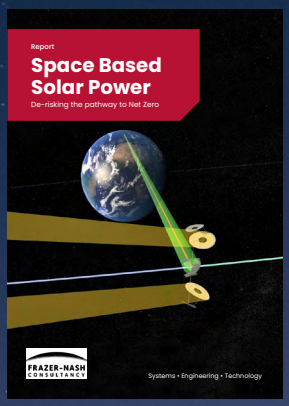
The potential benefits of SBSP are numerous, including national energy independence, increased grid resilience, and the ability to provide energy to remote areas and a being a key factor in reaching Net Zero. Nevertheless, given the global implications of new, large energy sources and the growing importance of politics and security in the space domain, it is necessary to consider the impacts SBSP might have on these areas.

In addition to considering the geopolitical and societal impacts to the security of SBSP, this paper will focus on the security considerations for a generic set of Operational Technology (OT) systems we anticipate an SBSP system would operate. Using this generic SBSP system, this paper considers the potential vulnerabilities of an SBSP system in terms of the consequences of an attack, the different malicious capabilities that could be deployed to target the generic SBSP system, the potential impact of these attacks and the types of mitigation that should be considered during the planning of a SBSP design programme to protect its system and make it more resilient.

Would you like to know more?

Our 2021 paper provides a techno-economic assessment of SBSP.

Click here >>



It is impossible to separate an SBSP system from broader geopolitical considerations. Which in this case include its impact on strategic and political issues in space (astropolitics), and international energy security.

The last few decades have seen the emergence of new players in space, both states and commercial actors, suggesting that this environment is not a 'sanctuary' immune to the competition and conflict common in all other domains. As access to space has become cheaper and more democratised [1], commercial entities are looking to maximise the potential benefits from acting in space. At the same time, space capabilities have become more important to all aspects of military and national security operations, with states more reliant than ever on space.

This has resulted in an associated increase in the proliferation of counterspace capabilities, ranging from cyber-attacks to kinetic Anti-Satellite (ASAT) missiles, that can deny, degrade or destroy space assets. Alongside this is an increase in hazards that result from a more congested orbital regime, such as potential collision between satellites or the estimated hundreds of thousands of pieces of debris in Low Earth Orbit (LEO).

Should an SBSP system be deployed and become operational, particularly if it is generating a significant proportion of a state's energy requirements, it will become a target for adversaries. Energy systems (such as the Nord Stream pipeline [2] and similar critical infrastructure [3]) have already been targets terrestrially as part of so-called 'greyzone' activities. Similarly, the conflict in Ukraine has shown that it is not only military space systems that can be affected. Civil and commercial space capabilities have fallen victim to attack [4] [5].

This suggests that an SBSP system, while ostensibly a civil capability that is providing a non-military benefit (at least not directly), cannot be considered immune to potential hostile activity.

In terms of societal implications, public perception is a critical factor that can influence SBSP's successful implementation. Drawing lessons from the rollout of 5G technology and other infrastructure projects, it is clear that proactive engagement, transparent communication, and comprehensive risk mitigation strategies (addressing safety and continuity of supply) are essential to address public concerns and build support for SBSP.

There will be understandable concerns about a new technology and its capabilities, including concerns about beaming microwaves from space to the ground station, and it should be anticipated that there will be questions about the impact on wildlife, people and technology that may be exposed to the beam. For example, what happens if a bird or passenger aircraft passes through the beam? What would be the impact on local communities and nearby transport networks?

Many infrastructure projects see disruption though direct action by activists, and while it is unlikely this can be prevented entirely, the ability to gain planning consent and the support of the general public will depend on the SBSP programme's ability to present easy to consume, verifiable information and evidence to support the safety of the system, and to counter any false claims circulated on social media. A failure to do may see a repetition of the problems seen with the roll out of 5G in the UK, with masts being damaged, protests at build locations and planning objections. Balancing the risks and benefits, while ensuring that community voices are integral to the decision-making process, can pave the way for the acceptance and integration of SBSP into the global energy landscape. While the planning consent process for a SBSP system are outside the bounds of this paper, it is important that security considerations are embedded within the process.

Our generic SBSP system

As with any strategic energy asset, it is likely that an SBSP system will become a target for groups that would seek to damage, degrade or deny the system's ability to deliver power to its customers, either for financial gain, or for political/strategic advantage. The system is also likely to attract espionage attempts looking to steal Intellectual Property (IP) or other key information or equipment.

The information assurance elements that would be used to protect IP/key information are likely to be the same as any organisation with IP and other sensitive information to protect, and this paper does not look at the details of the security of these systems.

The generic SBSP system has been considered as three main subsystems:

- **The In-Orbit Systems** – Consisting of a space solar array, and the construction/maintenance systems for the space solar array (we have excluded the launch and orbital transportation segments from this paper).
- **Ground station** – Consisting of the energy beam receiving rectenna, power conversion, grid connection, spacecraft control for the In-Orbit Systems, and supporting systems.
- **Up and down links** – Consisting of the systems used to communicate with the In-Orbit Systems, power beam targeting control, and a microwave power beam.

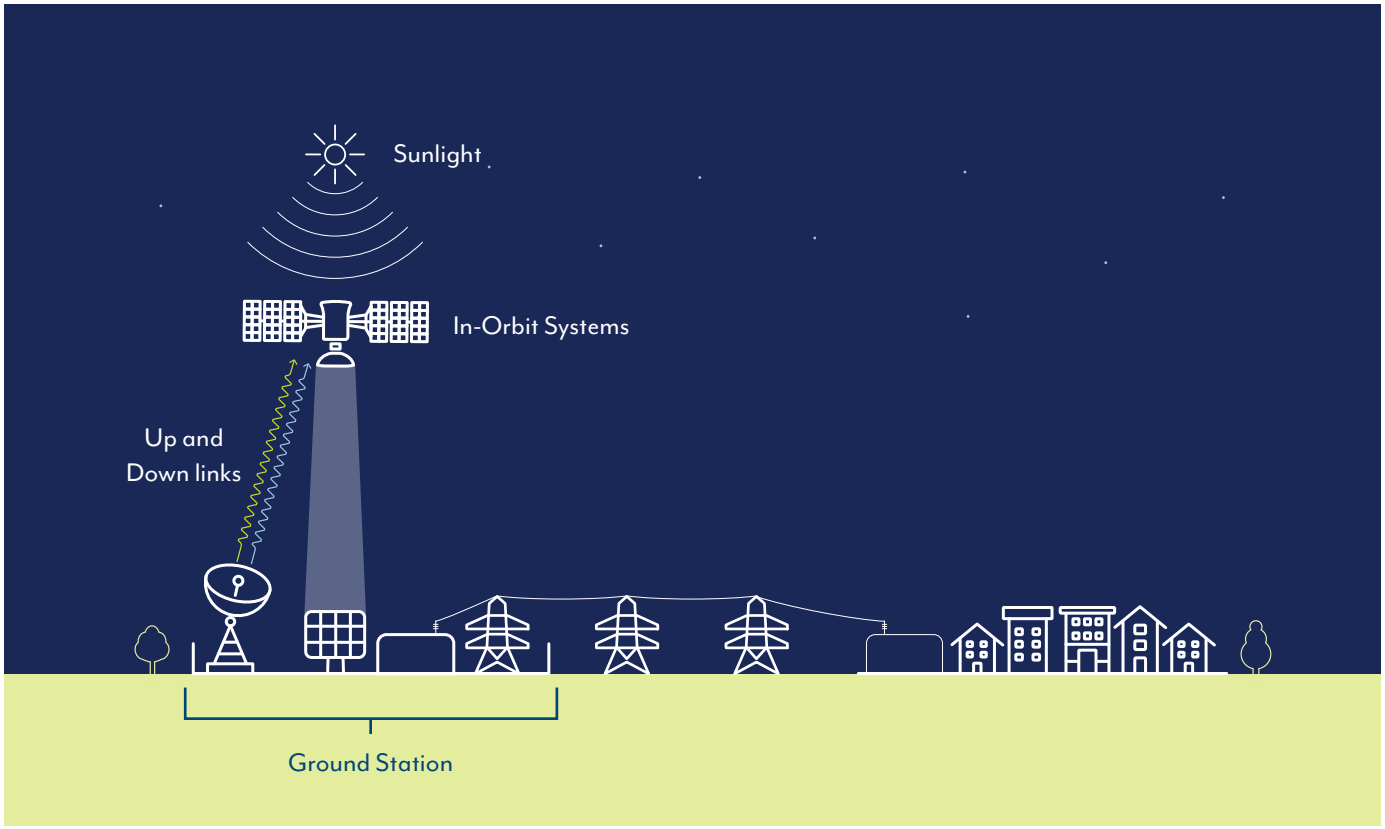


Figure 1 - High-level system view of our Generic SBSP system

Threat Actors

Nation states

The Intelligence Services/Military and Contractors of governments around the world are considered as potential threat actors. While the capability of each nation state varies, the most active Nation State threat actors targeting OT also have active space programmes. We have characterised Nation States with the following capabilities:

1. Rendezvous & Proximity Operations (RPO) [6].
2. Kinetic and non-kinetic Anti-satellite (A-SAT) capability [6].
3. Organised, advanced and persistent cyber capabilities targeting OT [7] [8].
4. Local intelligence assets/agents with the ability to access plant systems.

The rationale behind these types of threat would be for a nation state to disrupt the economic state of the country to gain an advantage, for example as part of a broader campaign of sub-threshold activity, to gain a strategic advantage through advancements in technology, and potentially to weaken an adversary's defence capabilities.

Organised criminals

These now make up a global industry, often with strong ties to nation states. Like nation states they can be well organised, persistent, and well-funded with advanced and persistent cyber capabilities (such as malware and ransomware) creatively making money from disrupting business including targeting OT [9].

Hacktivists/activists

Hacktivists have a political or social agenda against which they target their victims. Cyber security agencies such as the UKs NCSC and CISA have observed hacktivists targeting vulnerable, small-scale industrial control systems in North America and Europe [10]. These groups and individuals are currently limited to cyber operations to disrupt OT systems using malware, however their capability is growing. They may attack systems as a form of protest against any perceived environmental or ethical issues related to SBSP technology or perhaps to draw attention to issues of corporate control and energy equity.

Activists have a long history of interrupting and preventing organisations though physically preventing operations, this can include the blocking of roads, access to sites, digging tunnels in construction sites and using small boats to prevent offshore activity.

Insiders

Insiders can have rights that allow direct access to vital systems, they include the operators, maintainers, engineers and administrators of a system. Potential activity can result from malicious intent, such as sabotage or espionage, by individuals with access who steal or leak information to competitors, hostile nations or other malicious entities.

It could also be due to non-malicious intent by employees who are being bribed/blackmailed to use their access to release sensitive information. Alternatively, it could be through non-intentional accidental means by employees that use workarounds to "get the job done" or are unaware of correct process [11]. Insiders normally have access to many of a business's systems and the ability to make changes to OT systems (updating software, reconfiguring hardware, sending command signals, operating plant etc.). As such they represent a significant risk.

Our generic SBSP ground station is made up of the following structures and systems:

Enterprise IT systems

These will need to maintain the confidentiality, integrity and availability of the information systems. While important, the threats to these systems are well understood and not included here.

Ground station operational technology

It is anticipated that the following systems will contain operational technology on a SBSP ground station:

- Rectenna & beam control
  - » Pilot beam generation
  - » Pilot beam targeting
  - » Rectenna electrical protection
- Security monitoring and access control systems
- HVAC
- Maintenance systems
- Back-up power and ups
- Grid connection
- Temporary construction systems

The Spacecraft Control Facility will also contain OT:

- The actual space craft (see In Orbit Systems)
- The ground-based radio antenna
- Building management and HVAC
- Security monitoring and access control systems

Our generic ground station shows a single rectenna site, in practice this may be many rectenna sites located across multiple nations.

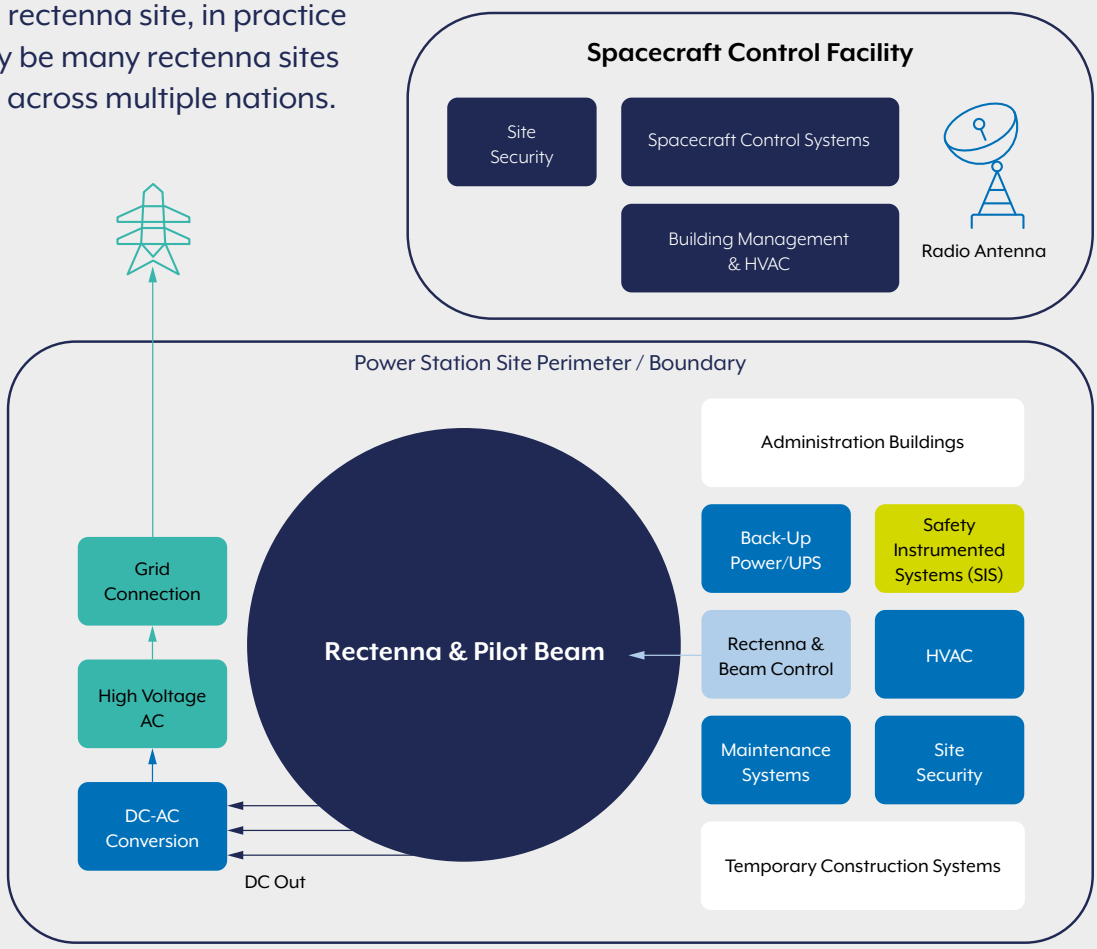


Figure 2 - Land-based Ground Station

Key areas of vulnerability

The following High Consequence events have been identified for a SBSP Ground Station, these events are presented here without mitigations which are discussed later in the paper:

- **Loss of safety protective systems** – This paper assumes that a small number of Safety Instrumented Systems (SIS) will be required to maintain the safety of personnel on site. If compromised the SIS may permit or cause a hazardous situation that could result in serious injury, death or environmental damage.
- **Loss of safety for third-parties** – The potential for people, animals and aircraft being exposed to the energy beam will give cause to safety concerns. Exposure may arise from them crossing into the beam or from a malicious or accidental movement of the beam. While the current beam technology in development is not expected to be hazardous[12] safeguards will need to be incorporated the maintain public confidence in SBSP.

High consequence events are those that result in unacceptable conditions for the asset owner or stakeholders in a SBSP system.

- **Loss of spacecraft control or key ground station systems**
  - » The representative ground station shown in Figure 2 includes systems that are used to control the in-orbit platforms including the build/maintenance systems and the SBSP spacecraft. The rectenna and spacecraft control systems are an easier option for most attackers to target compared to targeting the in-orbit system.
  - » Attackers may target the ground station to prevent operators from controlling the spacecraft and/or its build/maintenance systems, or they may choose to target other key systems used to operate or maintain the ground station.
  - » Attackers may target the ground station to attempt to change the direction of the power beam, change the beam intensity or change the spacecraft's flight path.
  - » Attackers may target the supply chain to introduce compromised code in patches or updates that are then sent via spacecraft control to the spacecraft. This may result in a remote access backdoor being added in or ransomware being uploaded.
- The key systems on the representative ground station in Figure 2 that attackers may target include the grid connection systems, such as electrical protection and metering systems, the stations back-up power systems, maintenance systems, HVAC that maintains environmental conditions of other key systems, and security systems such as access control and CCTV.

Key areas of vulnerability continued

Theft of critical systems/equipment

- There will be elements of the ground station technology that will be of interest to competitors, these may be targeted to allow others to access the IP/Trade Secrets within them.
- Some equipment will also hold information that would be of use to an adversary planning to attack the facility, system configuration data, IP addresses and architecture information may be held on devices that could be stolen, or accessed if devices are sent away for maintenance.
- There will be high value assets on the ground station, that may be targeted by organised crime for resale, particularly where there are long lead times on delivery both driving up desirability and the impact of any loss on an outage programme.

Significant design development delay/cost escalation

- The total loss of design data, or bespoke software during the latter stages of development would cause significant delay and/or cost while the work was repeated.
- The intrusion of threat actors into the software development environment may call into question the integrity of the software being developed. Assurance activities to prove the integrity of a system/software would be costly, cause delays and may ultimately fail.

Significant construction delay/cost escalation

- Attackers may target key systems used to build/ install or commission the ground station.
- Key construction OT systems may include concrete batching plants and specialist metrology systems and their data.
- There will be valuable elements of the ground station equipment and raw materials that may be targeted by organised crime during build for resale, particularly where there are long lead times on delivery both driving up desirability and the impact on any loss on the build or outage programme.
- Equipment/hardware supply chain infiltration and disruption/compromise, assembly of rectennas and SBSP satellites will require a continuous manufacturing, logistics and launch capability. e.g. Preventing the launch capability before a SBSP satellite is complete enough to begin revenue generation, or changing assembly lines to introduce latent defects that are only revealed in orbit.

Regulatory intervention

- A failure to meet licencing conditions though the non-compliance of security regulations would prevent an SBSP organisation launching and/or operating the spacecraft.

Relevant adversary capabilities

Malware

Ransomware

- Organised crime using specialist teams to assess potential victims, access their systems, target OT systems, wipe backup data, and deploy ransomware preventing the OT systems from operating/shutting down plant.
- This type of attack has seen massive growth of the last 5 years due to getting significant payouts, OT operators are a prime target.
- OT is often indirectly impacted when IT systems OT depends on are lost.
- It is also possible for state actors looking to deny the SBSP capability while avoiding attribution to use ransomware with no option to decrypt the compromised devices.

Damage

- Advanced malware has been used to target and damage control system hardware.
- Software updates + patches - these approaches provide initial access for other malware payloads such as those described so far.
- Watering hole attacks - where updates on vendor websites are infected and then downloaded by asset owners.
- The adversary infiltrates a software development environment in the supply chain and adds malicious code, such as the ability to remote access the compromised system.

Remote access

Data exfiltration

- Theft of IP and/or data that would be of use to an adversary.

Damage/risk to safety

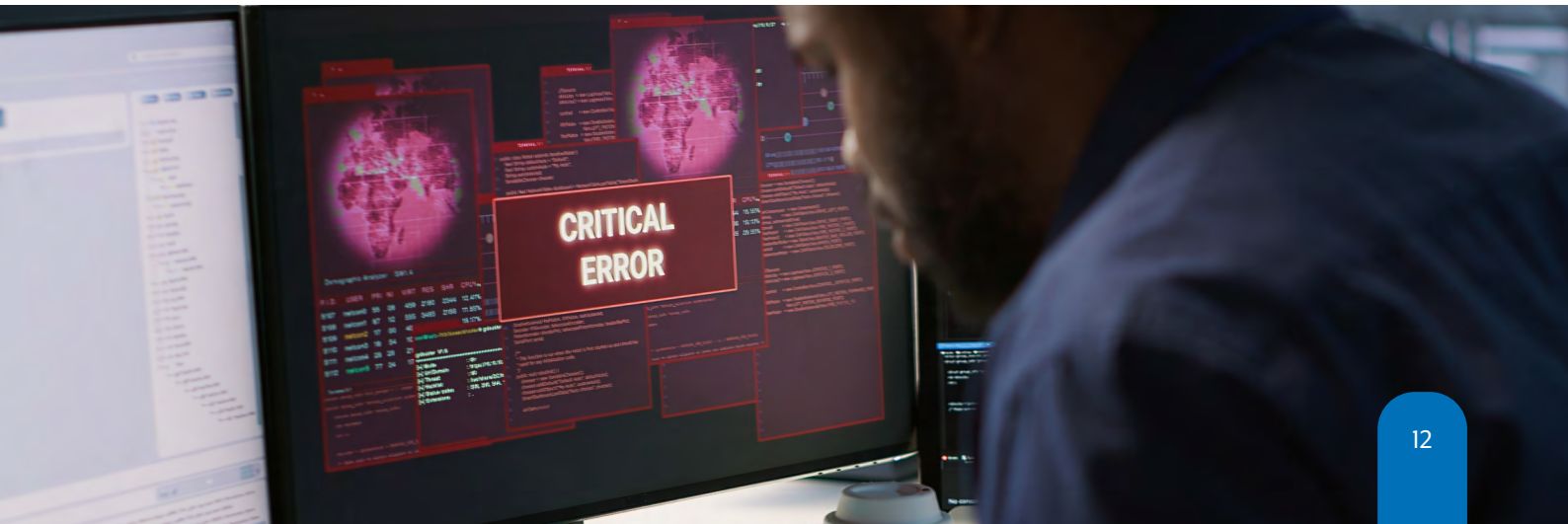
- There have been a number of attacks that have targeted:
  - » Electrical substations and other grid connections – causing blackouts.
  - » Safety Integrity Systems (SIS) attempting to cause an accident.
  - » Flooding/overflow of water treatment plants.
  - » Trip of plant operations.
  - » Toxic chemical dosing of water treatment plants.
- Even poorly conceived and executed penetration tests have caused downtime and physical damage to OT.

Physical access, damage and theft

Damage/removal of equipment during:

- Maintenance outages
- Offsite repair
- Protest incursion

Not all damage is obvious; any potential for interference, prepositioning of hardware could be problematic, and difficult to spot.



Ground Station – offshore

The offshore version of our generic ground station places the rectenna and local maintenance system on a floating platform and uses an undersea link to transfer power and data between the rectenna and the shore-based station.

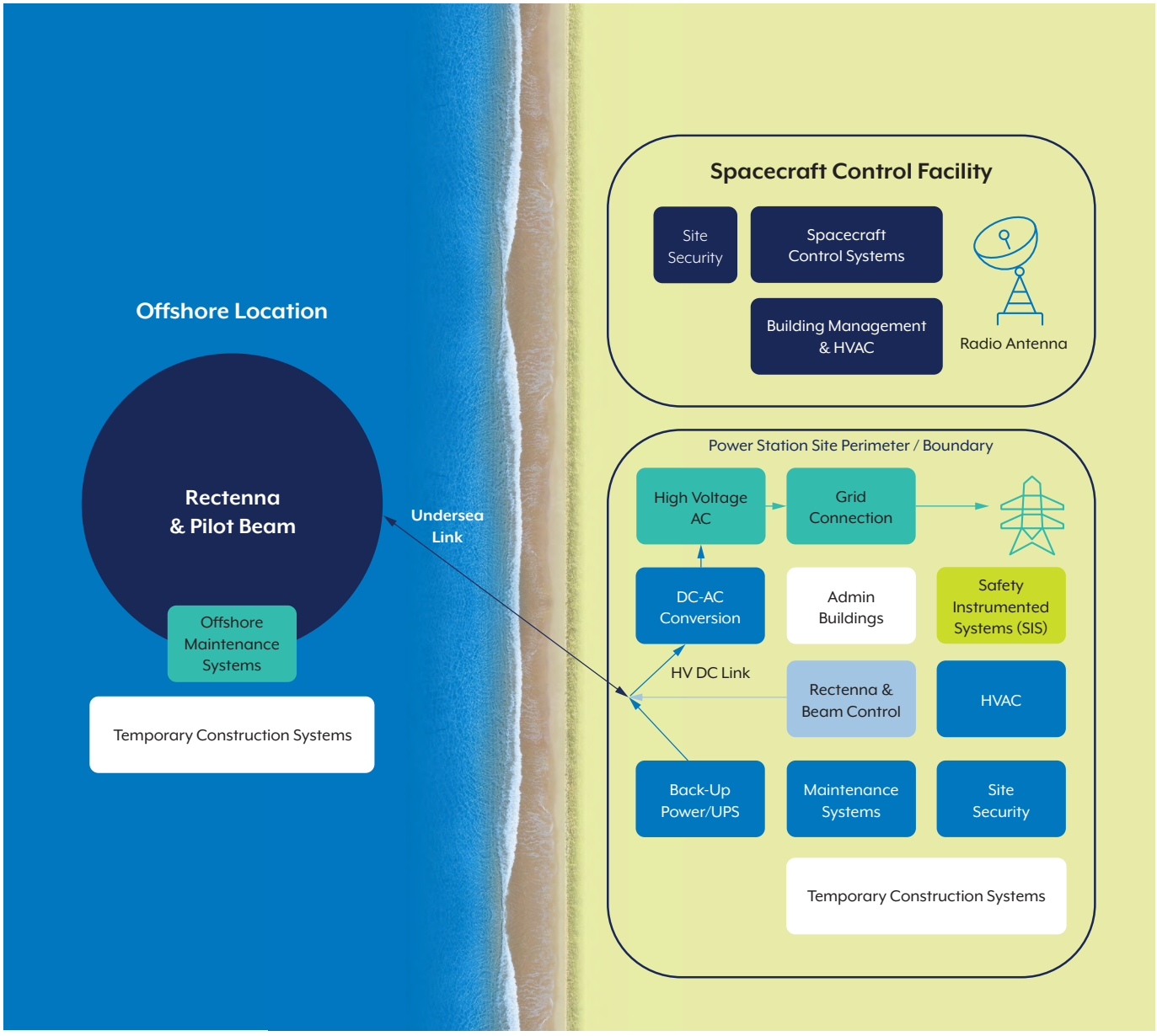


Figure 3 - Offshore Ground Station

Key areas of vulnerability

These will be the same as the land-based system with the following changes, again these events are presented here without mitigations which are discussed later in the paper:

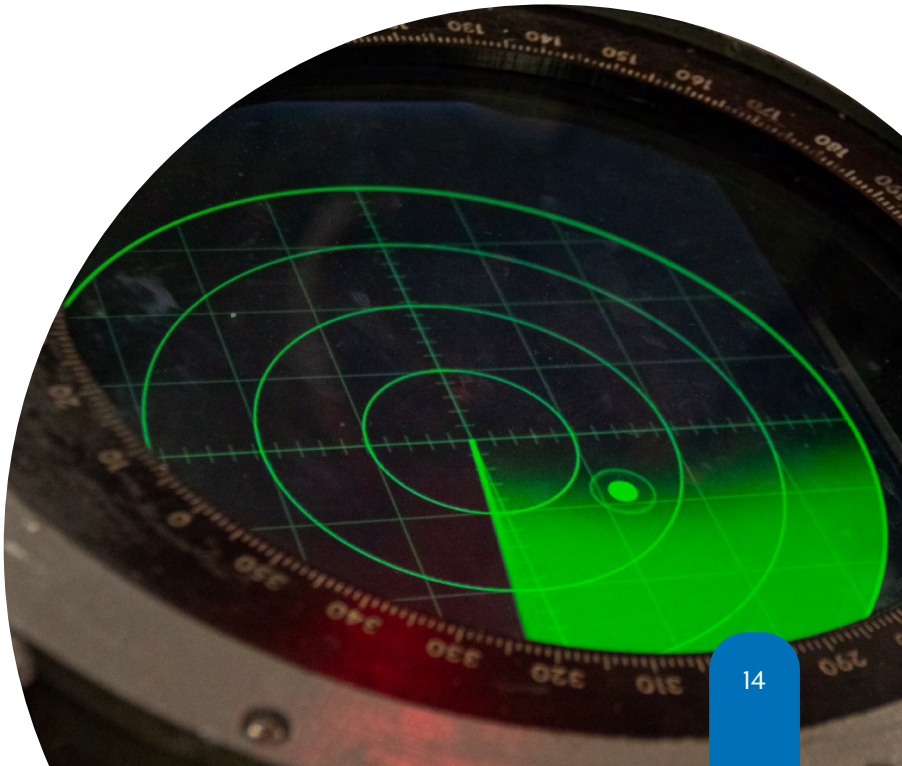
- Loss of spacecraft control or key ground station system
  - » The representative ground station with offshore rectenna shown in Figure 3 includes systems that are the same as the land-based system with the addition of a long undersea link and remote floating rectenna elements. As a remote off-shore system there will be additional risks due to acts of piracy or sabotage to the off-shore equipment or the undersea cable.
  - » Automation systems for operation and maintenance will likely all be accessed remotely, providing a greater attack surface.
  - » The offshore antenna will be more susceptible to protestors placing a small boat in close proximity to the rectenna, especially as an operator may be forced to shut down operations as a precaution (similar to runway or drone incursions at airports).
- Theft critical systems/equipment
  - » The entire off-shore system could be at risk of hijack or ransom (piracy) by a well organised criminal enterprise.
  - » Equipment could also be stolen from the platform during acts of piracy.

Relevant adversary capabilities

(In addition to those listed for the land-based system above)

Physical access, damage and theft

- Nation states and activist groups have demonstrated capability to damage offshore facilities and critical infrastructure [13].
- Acts of piracy are common but currently limited to certain locations. It is difficult to predict the attractiveness of this system as a target, but it should not be discounted.



Key areas of vulnerability

Figure 4 shows the typical connections in the communications conduit between the ground station and the in-orbit systems. The pilot beam is a signal sent from the rectenna up to the spacecraft to provide it with a bearing to direct the energy beam back to earth. Operational data represents the communications traffic used for system telemetry data, maintenance and construction instructions, system updates, along with any other information that needs to be exchanged between the ground based and in-orbit systems. These events are presented here without mitigations which are discussed later in the paper.

Loss of link

- Attackers may attempt to prevent communication and/or the pilot beam reaching the spacecraft by "jamming" the signal, this involves flooding the area around the link with Electromagnetic (EM)/ Radio Frequency (RF) noise, stopping the SBSP system from receiving the legitimate signal.
- Attackers may attempt physical blocking of the pilot beam using air or spacecraft placed between the rectenna and the spacecraft. While technically difficult to achieve its not implausible and could be difficult to counter.

Link compromised

- Attackers may setup a rogue uplink intended to overpower/takeover the command of the spacecraft.
- Attackers may attempt interception of the legitimate uplink/man in the middle attack to redirect the energy beam or takeover the control of the spacecraft.
- Attackers may attempt to compromise and take over the Legitimate Link by targeting the ground station (See Ground Station – Land).

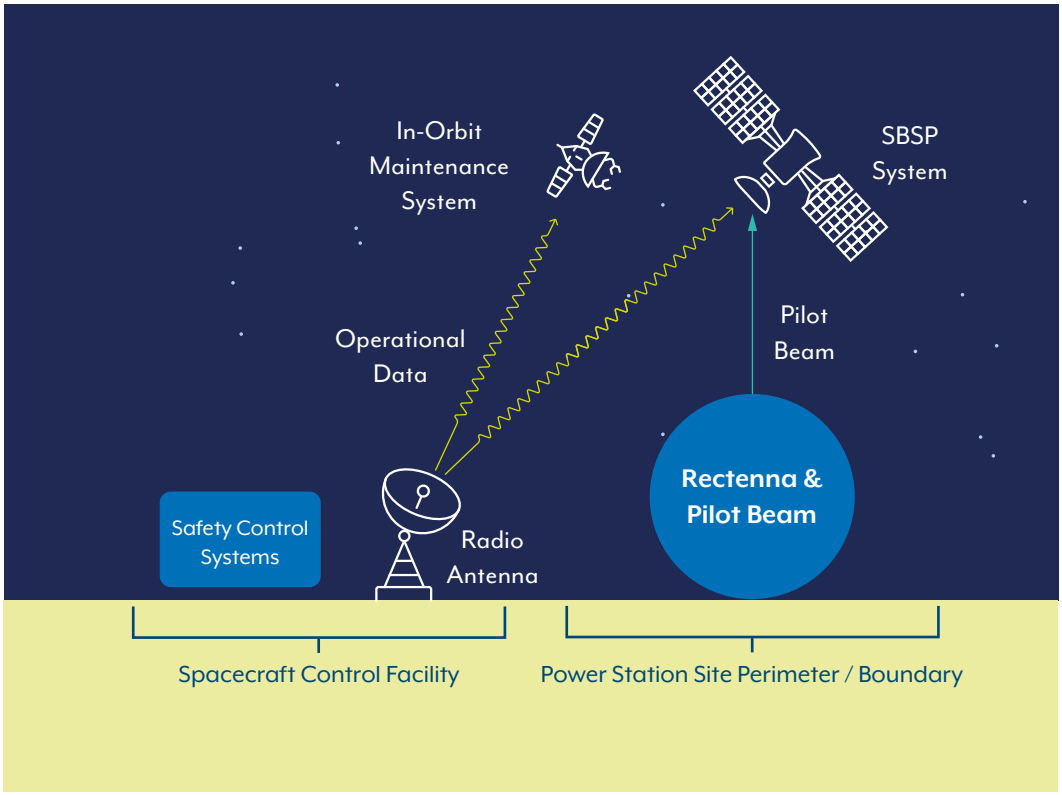


Figure 4 - Up and down links

Relevant adversary capabilities

Jamming

- This is a common and relatively low-tech threat to Radio Frequency (RF) communications that could be accidental or malicious, that could affect either end of the link.

Rogue transmitter

- With sufficient insider details on the link's communication protocol, authentication, frequency range, encryption, and power output, an adversary could imitate the uplink control signal and attempt to hijack control.

Blocking

- This would be limited to adversaries with access to specialised aircraft and spacecraft capable of holding station in the line-of-sight of the link. E.g. recently we have seen nation states using remotely operated balloons that in the future could be adapted to attempt this.

Intercept

- This would be a further evolution of the blocking capability to include data intercept, which could be used to then manipulate the SBSP system.

Ground station/up and down link summary

The system vulnerabilities and threats are shared with many other similar systems that either generate electricity or involve communication with satellites, this means that while SBSP is new, the threats are no worse than existing similar infrastructure and can be addressed using similar mitigations.

In-orbit systems

The in-orbit system will be made up of the following structures and systems as shown in Figure 4:

- The SBSP array – This will collect solar energy and convert it for transmission and then beam the energy to the ground station, the system will also perform communication and orbital light control activities.
- Construction/maintenance systems, these will be used to build the SBSP array, and are assumed to also support long term maintenance of itself and the SBSP array.

Key areas of vulnerability

The following High Consequence events have been identified for the in-orbit system:

Loss of spacecraft control

- Unauthorised Remote Access of the spacecraft. In addition to targeting the ground station (as previously discussed), attackers may attempt to directly communicate with the spacecraft to prevent legitimate access, for example they may directly upload malware such as Ransomware.

Control hijack

- Unauthorised Remote Access of the spacecraft. Attackers may attempt to directly communicate with the spacecraft to assume control. If successful they may attempt to redirect the energy beam, change its flight path, or change the beam intensity.

Damage and physical compromise

- An SBSP system will be in a known location, taking evasive actions will be difficult to do in operation, and it will be very big. All of this will make it vulnerable to physical attack.
- Weapons such as Direct Ascent ASAT missiles and Directed Energy Weapons may currently struggle to reach geostationary/geosynchronous orbit (GEO/GSO) [6], but it is likely that a capability could be developed by the time an SBSP system enters service. The scale of damage will be dependent of the weapon payload, and the scale and resilience of the SBSP system. Rendezvous & Proximity Operations (RPO) is a developing field [6], and it is likely that RPO will be more advanced, and utilised by more actors, by the time an SBSP system enters service.
- Rogue space craft. It is also possible that a spacecraft or debris collision either though accident or malicious intent could damage an orbital SBSP system.

Relevant adversary capabilities

Unauthorised remote access/malware

- Malware has been covered already in the ground stations however the requirement to communicate directly with a spacecraft in GEO/GSO is likely to limit adversaries to nation states.

Weapons such as Direct Ascent ASAT missiles and Directed Energy

- Direct Ascent ASAT weapons are limited to a small subset of nation states.
- Misfire of future terrestrial Directed Energy Weapons may also pose a threat to SBSP systems. It's possible that future energy beam weapons that are not affected by gravity could miss its intended target and damage/destroy an in-orbit system.

Rogue spacecraft

- In GEO/GSO, rogue spacecraft are more limited to a small subset of nation states and private enterprises, but with increases in launch capacity globally, the number of satellites in GEO/GSO is likely to increase.

In-orbit system summary

The in-orbit system vulnerabilities and threats are shared with many other similar in-orbit systems, this means that while SBSP is new, the threats are likely to be no worse than existing similar infrastructure and can be addressed using similar mitigations.

Future threats

With the deployment of full scale SBSP systems likely to be about 10-20 years away we also need to consider the potential future threat environment.

Cyber/technical threats

In the recent past we have seen the commercialisation of the threat, particularly with organised crime using ransomware to make significant sums of money, cryptocurrency tracing firm Chainalysis reported a record breaking $1.1 billion of ransoms paid in 2023 [14]. We are likely to see this trend continue, with ransom money being reinvested to build better tools, technology and skills in the criminal sector.

State actors will continue to target Critical National Infrastructure, building specific tools that target the operational technology used. Recent malware tools such as Pipedream are modular allowing them to be easily updated to target different hardware [15] [16] [17]. This is likely to continue with tools that target common traits/libraries shared multiple vendors of OT hardware.

Advancements in Artificial Intelligence (AI) are also lowering the bar for entry into attacking OT [18]. Commercially available generative AI (GenAI) is capable of teaching/helping users to understand OT hardware and how it works, and is also capable of producing simple python and shellcode that can be used maliciously [19]. There have also been attempts at producing malware [20]. Malicious actors will almost certainly be producing their own GenAI [18] that will not have the moral limitations set by the commercial versions. Over the next 10-20 years we should expect to see AI generated malware and more complex shellcode, all of which would be created by low skilled hackers. In addition the ability to use native shellcode elevates the unskilled hacker's ability to live off the land making it harder to detect them.

It's been well documented that quantum computing poses a potential threat to encryption [21], particularly the use of public key algorithms, and this would impact some forms of communications such as those used on SBSP to support secure communications with the spacecraft and direct the energy beam.

Some threat actors may collect encrypted data now with the intent to use future Quantum capability to access the critical information/intellectual property in the future.

The supply chain will continue to be a threat vector, especially as we see more integration of software, hardware and services (particularly cloud services). Threat actors will seek to inset their own malicious code into products, or add malicious hardware to equipment during design/production [22].

Remote hijacking of third-party spacecraft in orbit is of particular concern. The European Union Agency for Cybersecurity, ENISA, predicts that: *"By 2030, the space sector will likely transform even more with more investments of private actors, partnerships between private companies and governments, and increased geopolitical and commercial competition in space."* [22] ENISA goes on to say that there is a lack of security understanding, analysis and control of space-based infrastructure. Using ENISA's findings, we would anticipate that vulnerable spacecraft could be hijacked and used to collide with the SBSP platform.

As with many cyber attacks, remote hijacking is likely to be difficult to attribute. State actors will likely already have most of the capability to do this today but are not likely to be motivated to do so[2]. In 10-20 years it is likely that Hacktivists will also have the capability to attack vulnerable spacecraft, but unlike state actors may not be constrained by the same rules of engagement.

2. This is assumed given the risk of Kessler syndrome discussed in the mitigations later in this paper.

Physical threat

We are likely to see continuous development of counterspace capabilities that can physically impact space systems. Some of these will be based on existing technologies and capabilities that currently affect LEO and are thought to be able to affect GEO/GSO in the near and medium terms. Others are those that are at present theoretical but will potentially come to fruition during the lifetime of an SBSP system.

Many of these threats will continue to be the preserve of major state actors who have significant military space programmes. However, as technologies proliferate other actors, including minor space states, private companies and third-party actors (including proxies) could find themselves in possession of capabilities that could physically harm a satellite.

In particular, mention should be given to dual-use and dual-purpose capabilities that have not necessarily been developed with hostile intentions but could be used for such.

Areas of particular interest include:

- Earth based energy weapons that could reach GEO/GSO, especially if the beam can be sustained or cycled effectively to sweep across the target
- Co-orbital ASATs positioned in GEO/GSO with warheads developed for big structures, or SBSP technology (EMP, spread/spray of damaging/attenuating material)
- Increase in stealth capabilities for spacecraft
- Capabilities that could prevent solar energy from reaching the SBSP system
- Use/hijack of space assets and/or debris to cause physical damage
- Malicious or accidental misuse of centrifugal spacecraft launch catapults
- Threat from debris events elsewhere (can be non-malicious) – a monitor and clean function may be required for the orbital volume within a certain distance of the SBSP satellite, i.e. an ongoing live active debris removal (ADR) service.

It is of course impossible to predict the full nature of what capabilities may exist in the future that could cause physical harm, particularly due to the long life intended for an SBSP system. However, understanding the trajectory of current capabilities gives some idea of the types of threats that are likely to be applicable.

According to the European Space Agency. The Chinese FengYun-1C ASAT engagement in January 2007 alone increased the trackable space object population by 25%. [23]

Technical

The mitigations presented here are aimed at an organisation planning a programme for the design of an SBSP system. It should be noted that these mitigations should be considered in the context of risk to the programme at the time, for example these mitigations will not necessarily be applicable to demonstrator systems. A risk-based approach should be used to identify when mitigations should be adopted.

Regulation

There are regulatory and other frameworks that can be used. Embracing regulatory frameworks and building them into the SBSP organisations will help to deliver security within them and the SBSP systems they operate. In the UK, it is anticipated that three regulators will have an interest in SBSP:

- **In-Orbit Systems** – The CAA will have an interest in the launch systems, and the ability of the asset owner to operate a safe and secure space craft.
- **Ground station** – Ofgem are the energy regulator, and will be looking at the ability of the asset owner to operate as a licenced electricity company.
- **Up and down Links** – Regulated by Ofcom, for the most part it is anticipated that the security of the link will be regulated by one of the above regulators, while spectrum allocation is harmonised at an international level according to the International Telecommunication Union Radio Regulations, the UK regulator (Ofcom) will likely seek assurances that the power beam and other transmissions, even if compromised will not adversely impact other frequency bands.

The UK's NIS Regulations[3] are the basis for the regulatory framework managed by both the CAA and Ofgem using the Cyber Assessment Framework (CAF) produced by the UK National Cyber Security Centre (NCSC). While each regulator currently operates their own version of the CAF, they are fundamentally the same and incorporating them into a single CAF for a SBSP organisation would be trivial. They could then use their CAF to help them establish, audit and improve their security posture.

Given the potential international operating model where a single spacecraft serves multiple ground stations across the globe, it is likely that each ground station will need to conform to local cyber security regulation, and that the operating company will require an approach that satisfies the requirements of all the local regulators.

For the EU the relevant regulation is will be NIS 2.0 (a revised version of NIS that the UK has not adopted) and the European Cyber Resilience Act (CRA). The CRA describes the cybersecurity requirements for hardware and software products with digital elements placed on the market of the European Union, the benefit of CRA to SBSP developers is that SBSP components supplied from the EU will have to meet the CRA which will contribute towards their obligations under NIS 2.0.

The USA's North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan is a set of standards used for regulating the security of the Bulk Electric System in North America. These standards apply specifically to cybersecurity and provide a cybersecurity framework that we would anticipate being applicable to SBSP. The Federal Aviation Administration (FAA) regulates and licences commercial space operations. Cyber security standards are provided by the National Institute of Standards and Technology (NIST) such as the NIST Cybersecurity Framework (CSF) which can be used to support both ground and in-orbit systems.

It should be noted that most nations have some form of regulatory framework for the supply of energy and/or space operations that include security, it will be essential to understand the regulatory framework for perspective locations and plan to integrate them into the assurance programme of a SBSP system.

3. The UK NIS Regulations originated from the EUs NIS directive, however the UK are not adopting the NIS 2 directive but will be implementing their own updates to UK NIS.

Cyber Informed Engineering (CIE)

Cyber Informed Engineering (CIE) can be used to augment a secure by design approach by helping control system engineers/designers to integrate cybersecurity considerations into the conception, design, build, and operation of Operational Technology (OT) systems such as those used on a SBSP system.

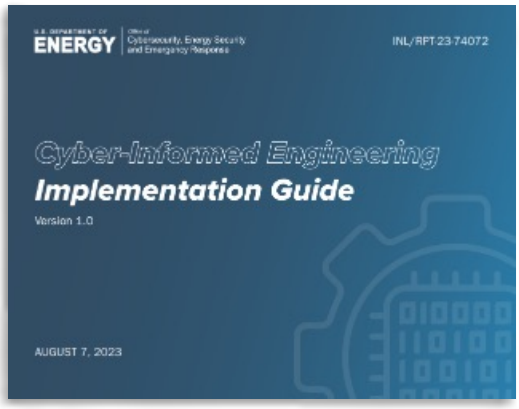
Sponsored by the U.S. Department of Energy (DoE) and developed by Idaho National Laboratory (INL) and members of an international CIE Community of Practice Implementation Working Group, the approach uses 12 design principles to help guide the development of any OT system (not just energy):

1. Consequence-Focused Design
2. Engineered Controls
3. Secure Information Architecture
4. Design Simplification
5. Layered Defences
6. Active Defence
7. Interdependency Evaluation
8. Digital Asset Awareness
9. Cyber-Secure Supply Chain Controls
10. Planned Resilience
11. Engineering Information Control
12. Organisational Culture

The CIE implementation guide [24] provides additional information to support an organisation in incorporating CIE into its engineering lifecycle from Concept design thorough to retirement and replacement. The implementation guide provides a set of questions for each phase of engineering lifecycle that relate back to the 12 design principles. Possibly the most powerful of the design principles is the first - Consequence-Focused Design[4], many security risk mitigation programmes start by identifying the security Threat, then the system's Vulnerabilities followed by the Risks and then defined some kind of risk treatment/mitigation.

The issue with this approach is that we need a system design to understand its vulnerabilities, and the further that design advances the harder it is to make effective changes to incorporate security controls and more costly those changes become.

With a Consequence-Focused Design approach it is possible to jump start the process by identifying consequences as soon as the hazards of a system



are identified i.e. at the HAZOP or PHA stage. INL have developed their own process for applying CIE at an organisational level, Consequence-Driven Cyber-Informed Engineering (CCE) [25] this defines a process of looking for High Consequence Events (HCE) that could have a critical impact on the organisation, this can also be applied at a system level where a HCE would result in unacceptable consequences to the asset owner.

By identifying a SBSP systems HCEs and relating them back to applicable OT systems it is possible to identify critical systems early in the design cycle and define appropriate security controls to help secure them (See Standards on next page).

Additionally as the design develops it is possible to inform the design of the systems with potentially unacceptable consequences using the CIE design principles to develop engineering grade[5] protections for a system that even if compromised cannot produce unacceptable consequences.

A further benefit of consequence focused design is that it is independent of the threat, if you can mitigate or accept the consequences to a tolerable level, a change in threat or threat likelihood such as those discussed in Future Threats should make no difference to a system using the CIE principles.

For design evaluation, we can borrow a powerful tool from the safety engineering discipline, the hierarchy of hazard controls. The UK's Office for Nuclear Regulation have adapted this into a hierarchy of security controls. Figure 6 shows the Secure by Design Hierarchy of Controls taken from the Security Assessment Principles for the Civil Nuclear Industry [26], this ranks the types of controls from those that are most effective at controlling a security risk to the least effective (and typically most expensive).

4. This paper is not an extensive explanation of the CIE principles but draws on relevant principles, it is however important to recognise that all 12 of the CIE design principles should be adopted to deliver a robust OT system.

Elimination

This is the removal of the risk, this could be engineering the system so that it is physically impossible for the beam intensity to exceed safe levels, or deciding not to have remote access to the OT system, however its often difficult to eliminate the risk without also removing key functionality of the system.

Substitution

Swapping a practice/device/system capability with an alternative that represents either no risk or a reduced risk, this could be replacing a software-based system with a hardware only solution that cannot be hacked, or replacing a firewall with a data diode.

Passive engineering controls

Using passive controls to secure a system, examples include architecting the system using of the perdue reference model to build a defendable network, and equipment hardening. It may also include designing flexibility into the system such as allowing communications links to upgrade/change encryption algorithms to combat any future weakness in encryption such as a cryptanalytic attack by a quantum computer.

A SBSP specific control could be to use the scale and distributed modular nature of a Gigawatt SBSP array to mitigate against Weapons such as Direct Assent ASAT missiles and Directed Energy Weapons. If each element of the array can capture and transmit energy, then if the remaining system architecture can be designed to be resilient to local area damage, the system would only be degraded not destroyed by this kind of attack.

Active engineering controls

Using controls that rely on an active security measure, Intrusion Detection systems, automatic access control, firewalls etc.

Operational/HF

These are controls that often manage/change the way people work, it relies on people following process and procedures, these may induce, scanning USB devices before plugging them in to plant computers, verifying the digital signature of a software update before patching a system, or posting signs for prohibited activity/devices in a secure zone.

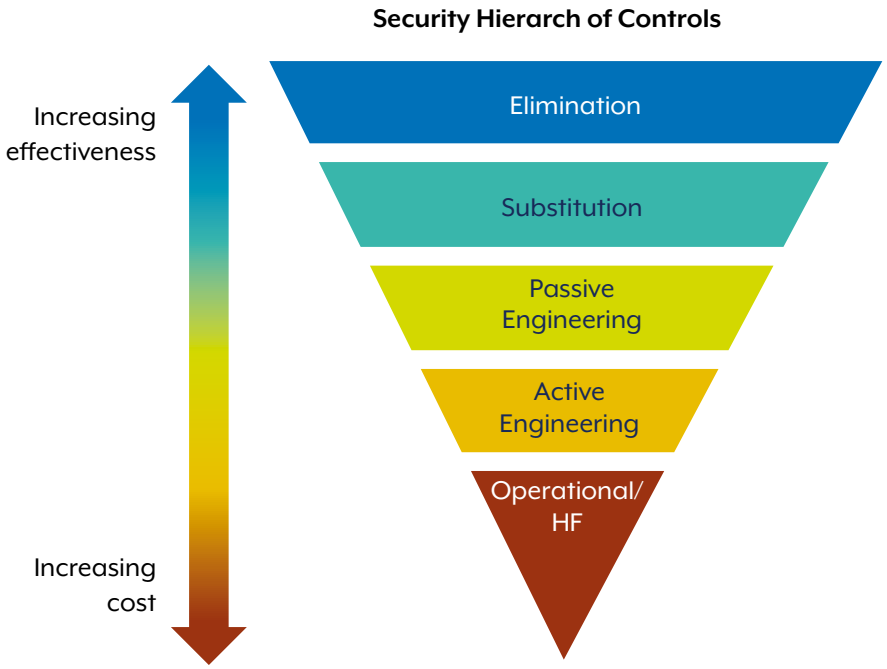


Figure 5 - Hierarchy of hazard controls

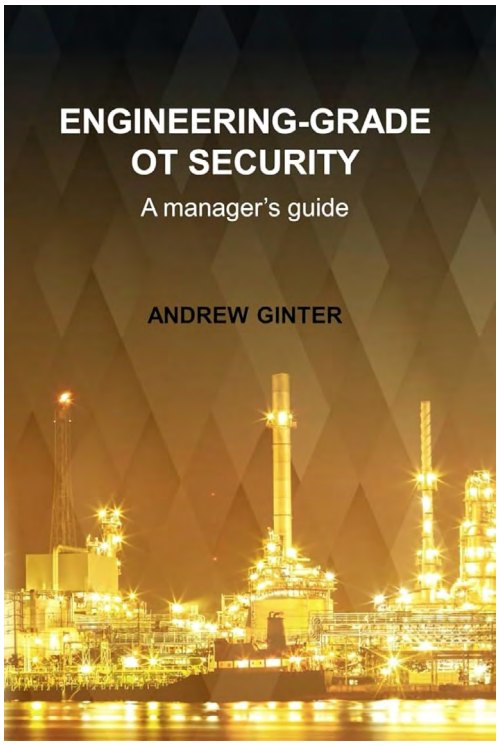
5. In this context, using protective devices that are not cyber vulnerable, e.g. are not dependent on software, or user/operator intervention for their protective function. These typically rely on physics to deliver the function, this approach is described in the next section.

Engineering grade protection

Engineering grade protections are an extension of the Elimination and Substitution controls in the hierarchy of security controls above. It involves using protective devices that are not cyber vulnerable, e.g. are not dependent on software or user/operator intervention for their protective function.

These typically rely on physics to deliver the function and are often changes to the design of the engineered solution to prevent unacceptable consequences occurring. Examples include adding a hardwired limit switch to a computer-controlled crane to prevent it from crashing into nearby items or using a pressure relief valve on a tank to prevent a computer-controlled pump from over pressurising it.

A recent publication Engineering-Grade OT Security A Managers Guide by Andrew Ginter [27] has bought together a number of these types of approach to form an introductory text of tools, technologies and process that can form the basis of a security engineering practice which can be built on to create engineering programmes that produce critical systems that are inherently secure.



Standards

For the in-orbit systems a SBSP operator will need to make security arrangements necessary to meet the requirements of an orbital operator licensee or similar according to their local regulatory framework, for the UK this will mean addressing the requirements of the Space Industry Regulations 2021 and the guidance provided in the CAA's CAP 2217.

For ground stations it would be beneficial to use a framework of internationally recognised standards which would help in the design of a generic station and then be adjusted if needed for local regulatory requirements. While some nations have well regarded OT cyber security standards that are widely adopted an international standard such as IEC 62443 would limit the possibility of clashes due to regional politics.

The SBSP programme will require a Cyber Security Management System (CSMS) to help in the setting up of the organisations security planning and governance, this can be achieved using IEC 62443-2-1 Part 2-1 - Establishing an Industrial Automation and Control Systems Security Program or NIST Cyber Security Framework (CSF) 2.0.

The various parts of the IEC 62443 standard provides guidance of the development and maintenance of OT (referred to as Industrial Automation and Control Systems - IACS) and incudes parts on the requirements on service providers, how to risk assess an IACS and sets out requirements at both the component and system level of the IACS.

The HCE assessment covered in the CIE section above fits well into this process as part of the initial risk assessment in part 3-2 of IEC 62443.

In-orbit defensive systems

The selection and design of in-orbit defensive systems would be a result of risk assessment and CIE processes. Defensive systems selection needs careful consideration to comply with regulation/treaty and to prevent unintended consequences.

This paper assumes that any kind of countermeasure cannot be considered an offense weapon to comply with regulation/treaty and to prevent the potential for creating debris, which in itself would pose a threat to SBSP. The following examples may be considered in the design process:

- **Collison avoidance** – Using a combination of space object tracking, and a propulsion system, the SBSP is moved to avoid incoming objects. This would rely on warnings with enough notice to evade the object. Designing a SBSP structure for GW scale satellites capable of handling the inertial forces of the evasive action, while still maintaining the power beam during the manoeuvre is significantly challenging. Providing sufficient propellant to sustain the evasive action, to deal with a deal with a rogue spacecraft capable of tracking and following the satellite also present challenges.
- **Jamming** – Would be a problematic mitigation, it would rely on an assumption a that an approaching rogue spacecraft is controlled remotely and has no autonomous or frequency hopping capability (which is unlikely) and may also be considered an offense weapon.
- **Rendezvous & Proximity Operations (RPO)** – The defensive use of RPO could be the use of semiautonomous drones to intercept and push away threats, it may also be possible to utilise the robotic maintenance systems to defend the SBSP system.

Ground and uplink defensive systems

These will be much the same as any critical national infrastructure asset, and so is not discussed here. It is worth noting that the CIE principals can be used to engineer out vulnerabilities, and risks such as limiting the beam's maximum power output to a level that is not harmful.

An area of emerging technology that is worth noting here is the use of semiautonomous drones to detect, deter and potentially defend an offshore platform while a rapid response is scrambled to the scene.

Insiders

To promote good security culture and reduce the insider vulnerability, there are a number of well-established mitigations that can be deployed such as vetting, segregation of duties and least privilege, this could be enhanced with appropriate culture for a given community e.g. focusing on good leadership, psychological safety staff physical and mental wellbeing, and inclusivity for the employees.

Geopolitical

We recognise that not all of the threats described can be mitigated by a technical means. Where this occurs, we anticipate that geopolitics and diplomacy will be essential to mitigating these risks. The threats we would seek to mitigate using this model include:

- ASAT capabilities
- Rendezvous & Proximity Operations (RPO)
- Other in-orbit activity that may be difficult to anticipate or attribute.

Treaty

The 1967 Outer Space Treaty [28] entered into force Oct. 10, 1967, and has 115 states-parties as of June 2024, with another 23 countries that have signed it but have not yet completed ratification. The parts that are relevant to a civil application such as SBSP are:

- *"Article III - States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding.*
- *Article VII - Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the earth, in air space or in outer space, including the moon and other celestial bodies."*

Convention on International Liability for Damage Caused by Space Objects [29], The Liability Convention agreement was reached in the UN's General Assembly in 1971, and the Convention entered into force in September 1972. The Liability Convention provides that the launching State is liable to pay compensation for damage caused by its space objects on the surface of the Earth or to aircraft, and liable for damage due to its faults in space.

It may also be beneficial for cooperating parties and even competing parties to enter into a SBSP agreement to establish a defined set of rules similar to the 1998 ISS agreement. This could be used to agree joint ownership of assets and utilisation rights to the power (similar to the ISS agreement) and foster a protected status for Critical National Infrastructure (CNI) in space with agreements of flight paths, orbits, dispute resolution and operational coordination, and could include measures such as sanctions for serious breaches.

International regulatory frameworks that provide a minimum standard for all space-based assets, this could be scalable to enforce security controls depending on the potential threat that an asset may pose to other assets should it be remotely hijacked.

Rules of engagement for directed energy weapons should also be investigated to prevent accidental/ collateral damage to SBSP platforms.

Within this area of geopolitical concerns, it is important for those developing SBSP systems to look at them not just from within their own frames of reference but also through different cultures that may have alternative approaches to space and energy security. The need for diverse voices within such discussions has gained prominence, ensuring that international conversations are not dominated by a Western point of view and include representatives from different backgrounds. This is also important when considering the sharing of the power gathered from an SBSP system especially where there are uneven power dynamics or, it could be perceived as colonialism.

Power supply diplomacy

One of the key benefits of SBSP is that the in-orbit platform could service multiple ground stations, for example, depending on the orbit, the UK could potentially share its SBSP capability with parts of South America, Africa, Easten Europe or Western Asia as peak demand in the UK reduced. This sharing of infrastructure would give the users of the platform and their allies a vested interest in its safety, and security. It may also help to encourage additional signatories of the 1967 Outer Space Treaty [28].

Kessler syndrome

A kinetic attack on a spacecraft the size of an in-orbit SPBP system is very likely to cause large amounts of debris collisions, this could lead to a cascade in which each collision generates space debris that increases the likelihood of further collisions (Kessler syndrome). This would cause a significant hazard to other assets in GEO/GSO and possibly LEO making some orbits/rejoins of space unusable.

In addition to this type of attack being a breach of the 1967 Outer Space Treaty [28], all of the nations capable of targeting a platform in GEO/GSO have their own assets in orbit and may even have their own SBSP programme. It is arguable that they would see a kinetic attack as too much of a risk to their own assets and aspirations due to Kessler syndrome.

Tracking and attribution deterrent

Capabilities such as KBR's Iron Stallion provide the ability to detect, monitor, track and report on the movement of objects in space [31]. In addition to real time monitoring and alerts for space-based objects that could pose a threat to an SBSP spacecraft, having a capability to track the origin of those threats would provide a deterrent as potential threat actors would know they may be sanctioned for their actions.

Conclusions

As discussed in the Geopolitical and Societal Considerations above, SBSP systems are likely to be targeted by well-funded and organised adversaries across the life of the plant, however, the security risks posed to SBSP are the same as other critical national infrastructure assets. The SBSP community can benefit by adopting existing established approaches to security and engaging in the mitigations described in this paper. Security is achievable and required for safe and reliable SBSP power stations.

The themes touched on in this paper show that there is benefit to early engagement with security to help eliminate and substitute security risks in the design of the system. Incorporating Cyber Informed Engineering (CIE) into the development programme will augment standards like IEC 62443 and help to deliver inherently secure OT systems with engineering grade protections.

The use of diplomacy will be essential to unlock the SBSP potential, as will the use of collaborative international agreements to establish a mutually beneficial frameworks for building, operating and protecting SBSP platforms combined with tracking technology to monitor compliance will help to mitigate the risks.

Public engagement will be essential to reduce the risk from activist causing harm, disruption and intimidation at ground-based sites.

Recommendations

RECOMMENDATIONS	WHO SHOULD BE INVOLVED	TIME SCALES
Adopt Cyber Informed Engineering (CIE) methodology for the design, build and operation of SBSP.	SBSP developers and the owners of SBSP assets.	This will apply to the whole life of a SBSP system, starting during the initial design stage.
Applying CIE Engineered Controls to consider the size and construction of the in-orbit systems in mitigating security threats: • **Collision avoidance with a single large gigawatt system may be difficult to achieve, but a constellation of smaller megawatt systems may provide the same overall power while being easier to manoeuvre and providing resilience against a single in-orbit system failure.** • **Accept that single large gigawatt system will be periodically struck and build resilience into the design e.g. modular independent systems that support a damage tolerant architecture that also limits debris generation and the possibility of localised Kessler syndrome.**	SBSP developers and the owners of SBSP assets.	The design decisions will need to be made early in the development of the system, however supporting research/ modelling will be needed in advance to understand the mechanics of SBSP debris.
Use internationally recognised standards such as ISA/IEC62443 for the cyber security of the OT systems.	SBSP developers and the owners of SBSP assets.	This determination should be made during at the start of the development programme.
Use a design risk assessment process to integrate appropriate risk mitigations and defensive systems into the SBSP design.	SBSP developers and the owners of SBSP assets.	The risk assessment process should be conducted at key stages of the design, starting at concept and then again prior to detailed design.
Plan to use regulatory frameworks like NCSC's CAF or NIST CSF and engage with regulators early.	SBSP developers and the owners of SBSP assets.	This determination should be made during at the start of the development programme.
Build international consensus with a 1998 ISS agreement style SBSP Agreement.	Governments seeking to have a SBSP industry, space agencies, SBSP developers and the planned owners of SBSP assets.	This work is necessary to de-risk SBSP programmes and will help to unlock investment, therefore it should start now.
Agree international regulatory frameworks that enforce security controls for all space-based assets to prevent their remote hijack.	Governments seeking to have a SBSP industry, space agencies, SBSP and other space craft developers and the planned owners of space assets.	This work is necessary to de-risk SBSP programmes and will help to unlock investment, therefore it should start now.

RECOMMENDATIONS	WHO SHOULD BE INVOLVED	TIME SCALES
Build multinational partnerships to share energy from SBSP assets.	Governments seeking to have a SBSP industry, electricity grid owners, SBSP developers and the planned owners of SBSP assets.	This work is necessary to de-risk SBSP programmes and will help to unlock investment, therefore it should start now.
Invest in high resolution space object tracking capabilities that supports attribution of RPO and kinetic attack.	Governments seeking to have a SBSP industry and space agencies.	Assuming SBSP starts to place critical assets in orbit in the next 10 years then this capability (both the technology and the operator ability) needs to be enhanced and matured by then.
Develop defensive RPO capability to defend the in-orbit systems.	Governments seeking to have a SBSP industry, space agencies, SBSP and other space craft developers and the planned owners of space assets.	Assuming SBSP starts to place critical assets in orbit in the next 10 years then this capability (both the technology and the operator ability) needs to be enhanced and matured by then.
Develop International Energy Weapon rules of engagement, to prevent assets being "down range".	Governments seeking to have a SBSP industry, international militaries and space agencies.	This should be developed in step with the energy weapon capability.
Learn lessons from the 5G rollout and other construction projects to minimise activist harm.	SBSP developers and the owners of SBSP assets.	This should be completed with action plans in place prior to any public beam testing.
Use supply chains that can demonstrate their OT cyber security arrangements, and monitor for Counterfeit, Suspect and Fraudulent Items (CSFI).	SBSP developers and the owners of SBSP assets.	During supplier selection.
Consider using post-quantum encryption now for any information that needs to be protected in the long term.	SBSP developers and the owners of SBSP assets.	Transitioning to post quantum cryptography should be planned into organisation's governance policy now.
Insider vulnerability management by fostering an appropriate culture for the organisation to reduce the vulnerability factors, such as a culture of wellbeing, good leadership and psychological safety.	SBSP developers and the owners of SBSP assets.	This should be in place at the start of the development programme and maintained for the life of the SBSP system.
SBSP operators should maintain awareness of the developing space and energy threat landscape for the life of the system.	SBSP developers and the owners of SBSP assets.	This should be in place at the start of the development programme and maintained for the life of the SBSP system.

References

[1] H. W. Jones, "The Recent Large Reduction in Space Launch Cost," in *48th International Conference on Environmental Systems*, Albuquerque, New Mexico, 2018.

[2] BBC News, "Nord Stream leaks: Sabotage to blame, says EU," BBC, 28 September 2022. [Online]. Available: https://www.bbc.co.uk/news/world-europe-63057966. [Accessed 16 August 2024].

[3] CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[4] Wired, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," Wired, 23 March 2022. [Online]. Available: https://www.wired.com/story/viasat-internet-hack-ukraine-russia/.

[5] The New York Times, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service," [Online]. Available: https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

[6] V. Samson and B. Weeden, "Secure World Foundation," April 2020. [Online]. Available: https://swfound.org/media/206957/swf_global_counterspace_april2020_es.pdf. [Accessed 3rd May 2024].

[7] CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," 7th February 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. [Accessed 3rd May 2024].

[8] CISA, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities," 1st December 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a. [Accessed 3rd May 2024].

[9] A. H. Alamri, "Dragos Industrial Ransomware Analysis: Q1 2024," Dragos , 25th April 2024. [Online]. Available: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2024/. [Accessed 3rd May 2024].

[10] NCSC, "Heightened threat of state-aligned groups against western critical national infrastructure," NCSC, 1st May 2024. [Online]. Available: https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups. [Accessed 3rd May 2024].

[11] CISA, "Defining Insider Threats," [Online]. Available: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats. [Accessed 3rd May 2024].

[12] The Europeran Space Agency, "FAQ: Frequently Asked Questions on Space-Based Solar Power," ESA, [Online]. Available: https://www.esa.int/Enabling_Support/Space_Engineering_Technology/SOLARIS/FAQ_Frequently_Asked_Questions_on_Space-Based_Solar_Power. [Accessed 30 Aug 2024].

[13] BBC News, "Ukraine war: The Russian ships accused of North Sea sabotage," BBC, 19 April 2023. [Online]. Available: https://www.bbc.co.uk/news/world-europe-65309687. [Accessed 19 August 2024].

[14] Chainalysis, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," Chainalysis, 7 February 2024 . [Online]. Available: https://www.chainalysis.com/blog/ransomware-2024/. [Accessed 17 07 2024].

[15] Dragos, "CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)," Dragos, 13 April 2022. [Online]. Available: https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/. [Accessed 17 07 2024].

[16] Dragos, "PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS," April 2022. [Online]. Available: https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf?hsLang=en. [Accessed August 2024].

[17] CISA, "APT Cyber Tools Targeting ICS/SCADA Devices," CISA, 25 May 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a. [Accessed 17 07 2024].

[18] NCSC (UK), "The near-term impact of AI on the cyber threat," NCSC, 24 January 2024. [Online]. Available: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat. [Accessed 17 July 2024].

[19] PC Mag, "https://uk.pcmag.com/ai/151797/an-ai-chatbot-may-have-helped-create-this-malware-attack," PC Mag, 10 April 2024. [Online]. Available: https://uk.pcmag.com/ai/151797/an-ai-chatbot-may-have-helped-create-this-malware-attack. [Accessed 17 July 2024].

[20] Tom's Hardware, "FBI: AI Makes it Easier for Hackers to Generate Attacks," Tom's Hardware, 30 July 2023. [Online]. Available: https://www.tomshardware.com/news/fbi-warns-about-ai-attacks. [Accessed 17 July 2024].

[21] Science.org, "'Surprising and super cool.' Quantum algorithm offers faster way to hack internet encryption," 09 September 2023. [Online]. Available: https://www.science.org/content/article/surprising-and-supercool-quantum-algorithm-offers-faster-way-hack-internet-encryption. [Accessed 17 July 2024].

[22] European Union Agency for Cybersecurity, "ENISA Foresight Cybersecurity Threats for 2030," 29 March 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030. [Accessed 18 July 2024].

[23] Source: https://www.esa.int/Space_Safety/Space_Debris/About_space_debris

[24] Idaho National Laboratory (INL), Cyber-Informed Engineering Implementation Guide, Idaho Falls: Idaho National Laboratory (INL), 2023.

[25] A. A. Bochman and S. Freeman, Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE), CRC Press, 2021.

[26] Office for Nuclear Regulation (ONR), "Security Assessment Principles (SyAPs)," 2022. [Online]. Available: https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/security-assessment-principles-syaps/security-assessment-principles-syaps/. [Accessed 20th May 2024].

[27] A. Ginter, Engineering-Grade OT Security A Managers Guide, Calgary: Abterra Technologies Inc., 2023.

[28] United Nations, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," United Nations, [Online]. Available: https://treaties.unoda.org/t/outer_space. [Accessed July 2024].

[29] United Nations , "Convention on International Liability for Damage Caused by Space Objects," United Nations, [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html. [Accessed July 2024].

[30] Frazer-Nash Consultancy, "Space Based Solar Power: De-Risking the Pathway to Net Zero," 2021. [Online]. Available: https://www.fnc.co.uk/discover-frazer-nash/news/frazer-nash-report-for-uk-government-shows-feasibility-of-space-solar-power/.

[31] KBR Inc, "Iron Stallion," [Online]. Available: https://kbr.foleon.com/gs-us/ironstallion/. [Accessed 29 04 2025].

About the Authors

Charlie Hall

Charlie is an industrial Cyber Security specialist focused on critical national infrastructure. With a strong background in developing high integrity Electrical, Control, and Instrumentation (EC&I) systems, Charlie has contributed to numerous projects in the Nuclear, Defence, and Aerospace sectors, both in the UK and internationally.

Ali Stickings

Ali is an expert in space safety, security, and sustainability, with a background in UK and international space policy and strategy. Ali has collaborated with militaries, governments, industry, and the non-profit sector on a wide range of space projects and initiatives.

Heather Taylor

Heather is a psychologist and behavioural scientist specialising in the behavioural aspects of cyber security and AI. She collaborates closely with government, defence, and industry on various projects, ensuring human considerations are integral to system design and implementation.

We'd love to connect with you to discuss the paper, SBSP or anything space or security related! You can do this by scanning the QR's codes which will take you to our LinkedIn profiles.

FRAZER-NASH CONSULTANCY
A KBR COMPANY

Frazer-Nash Consultancy Ltd
Hill Park Court
Springfield Drive
Leatherhead
Surrey
KT22 7NL

T +44 (0)333 032 9500

fnc.co.uk