Threat modelling helps you identify your cyber risks. Critical assets are data or functions where a loss of confidentiality, integrity or availability would result in a significant negative impact to stakeholders.

Identify Critical Assets → Understand Who Might Attack Them → Understand How They Might Attack Them

Potential Impacts of Cyber-Attacks on Smart Streets	
Severe traffic disruption leading to economic damage and potential loss of life in case of delay to emergency services	Major denial of service to local transport due to disruption to electric vehicle charging
Loss of income from fees, tolls, fines, fares etc.	Public exposed to additional safety hazards
Increased emissions	Loss of reputation
Fines of up to £18m for unsecure management of personal data	Losses due to being unable to supply contractually agreed data to support private partners

The NCSC advises local authorities to consider the types of threat actors that pose risk to them. From a smart streets perspective, these are some of the key threat actors authorities should consider:

Threat Actors	Motivation and Capability
Mischievous Amateur	• The ability to cause disruption in cyber-physical spaces such as smart streets is appealing to amateur hackers given the potential real-world impacts and likely media coverage. • However, such amateurs tend to have limited resources and skills. They tend to use simple, widely known methods that are well documented online to attack blatant security flaws (low hanging fruit).
Innocent Insider	• Innocent insiders may accidentally facilitate cyber-attacks against smart street systems. These are commonly system maintainers who accidentally introduce malware while trying to diagnose or resolve system issues or perform routine maintenance. They may also be system users. • Innocent Insiders are most likely to become threat actors when they have an insufficient appreciation of cyber security risks and how to protect against them.
Malicious Insider	• A malicious insider is generally driven by grievances or by a desire for financial gain. Malicious insiders tend to have limited experience of exploiting cyber security vulnerabilities. • However they will usually have a high level of access to systems and a better understanding of those systems than most. Malicious insiders can be particularly dangerous when teamed with a sophisticated external attacker.
Hacktivist Group	• Hacktivists are those that use cyber-attacks to further their political or philosophical interests. Road transport has been targeted significantly by activists in recent years, and increased connectivity could expose smart streets to hacktivists as well. • The capability of hacktivists tends to be greater than that of amateurs, and they tend to be able to gain greater insider knowledge by leveraging connections.
Organised Crime Group	• Organised criminals are primarily interested in financial gain and tend to use ransomware techniques to exploit their victims. Given that smart street services tend to be important to the local economy as a whole, cyber criminals may identify smart streets as a potentially lucrative target. • However, local authorities can fall victim even when not targeted. For example, speed cameras in Melbourne were taken offline by WannaCry despite the fact that it was not specifically targeted at transport. Organised cyber-criminals are becoming increasingly more sophisticated given the significant amounts of money involved.
State-Sponsored Hacking Group	• State-sponsored hacking groups are highly sophisticated attackers with significant resources. Their motivations are steered by governments hostile to or in strategic competition with the United Kingdom. • State-sponsored hacking groups tend to quietly search for vulnerabilities in systems that allow them to build a persistent presence on the network and research operations and technologies. They may use the access and knowledge built over time to eventually deliver a critical attack. • In the smart streets industry, this would likely aim to cause disruption or safety risks and demoralise. During the Russo-Ukrainian War, such groups have used cyber-attacks to damage the ability of the opposing nations to deploy troops and equipment.

Following the widely used STRIDE model for identifying cyber security threats, these are the types of attacks against a smart street system you should consider. These attacks attempt to violate certain desired system properties.

Attack Types	Violated Property
Spoofing	User/Service Authentication
Tampering	Data/Communication Integrity
Repudiation	Non-Repudiability of Actions
Information Disclosure	Data/Communication Confidentiality
Denial of Service	Service Availability
Elevation of Privileges	User/Service Authorisation

Considering typical critical assets in smart streets solutions, these are common threats a local authority might consider:

Threats	Example Case
Compromise of third-party cloud service provider (resulting in a loss of availability or integrity of the data streams used to run smart street services)	A local authority's traffic light timing is automatically optimised based on live vehicle traffic information. The traffic data is processed by a supplier's software running on a third-party cloud. The cloud service provider is attacked goes offline. As a result, traffic optimisation service is lost. Traffic jams significantly increase in the local authority area with potential knock-on effects on surrounding areas.
Systems unknowingly exposed to internet	Some smart street systems may be unknowingly exposed to the internet, either due to misconfiguration or inadequate security measures. Attackers can exploit these vulnerabilities to gain unauthorized access to the system and steal data or disrupt services. For example, CCTV cameras connected over 4G and misconfigured to use a public APN can be connected to by malicious parties over the internet.
Malware on removable media devices	A maintainer decides to charge a mobile phone using a free USB port while working on smart street infrastructure. The mobile phone is compromised with malware, and that malware infects the smart street component. Or the maintainer is deploying an updated configuration to a smart street system and uses an infected USB drive to transfer the data.
Data exfiltration from smart street systems	In 2020, Sheffield City Council's ANPR system, which contained 8.6 million driver records covering private journey data, was compromised by security researchers. The incident highlighted the risk of data exfiltration from smart street systems, where sensitive data can be stolen and sold on the dark web or used for other malicious purposes. This could result in significant harm to individuals' privacy, identity theft, and potential financial losses. It could also damage the reputation of the local authority and erode public trust in their ability to secure sensitive data.
Unauthorised physical access to smart street infrastructure	Many smart street infrastructure components are geographically dispersed and can be physically accessed in a discreet manner. With physical access, an attacker may find it easier to execute attacks that bypass layers of security placed between the system and the internet (including an air gap). An attacker could spoof a component on an internal network and gain more privileged access. This can be used to inject unauthorised data and commands into the system or exfiltrate sensitive data like individual vehicle movements.
Smart street components compromised in the supply chain (or otherwise vulnerable components procured)	A CCTV camera being used by the local authority has been designed and manufactured by a supplier that is obligated to engineer in security weaknesses or provide data or backdoor access to a foreign government. This is exploited to give an attacker a presence on the smart street system network.
Unauthorised access to remote monitoring, management and/or maintenance interfaces	A local authority sets up a VPN that allows maintainers to connect into the traffic management network using their laptop so they can monitor, configure and maintain equipment regardless of their physical location. The VPN uses a shared password and lacks multi-factor authentication. The credentials are compromised when LA staff use email to share the details with a new starter. An attacker connects to the VPN and reconfigures equipment to cause traffic disruptions, display misleading messages on signs, etc.
Ransomware attacks	The parking payment system is attacked with ransomware, meaning that the local authority cannot collect payment for any parking. As a result, the authority loses significant income and parking becomes chaotic, disrupting businesses and upsetting residents.
Social engineering attacks targeting smart street personnel	An attacker sends a phishing email to a local authority employee responsible for managing the smart street user data (e.g. for parking, fines, etc.), pretending to be a supplier and asking for access to the system. The employee unwittingly grants access, allowing the attacker to take control of the system and potentially cause widespread disruption or unauthorised personal data release.
Manipulation of data or information	An attacker could manipulate traffic sensor data to create the illusion of a traffic jam, causing drivers to take unnecessary detours or causing additional congestion. Such an attack has previously been demonstrated against mobile phone-based traffic monitoring systems.
Malicious data provided to ITS by third-party consumer apps	In 2020, researchers hacked Dutch cycling apps that were connected to traffic control systems operated by local authorities. By using modified versions of the apps, they were able to remotely trigger traffic lights across the Netherlands. This could cause widespread disruption and potential safety hazards for drivers and pedestrians alike.