An Introduction to the Political, Economic and Social Impacts of a National Cyber Security Incident

Contents

Overview

Module Description and Aims

Commented [RD1]: Paraphrase and edit for the handbook

This module has primarily been developed to further enhance the skills of the learners to take part in, for example, cyber competitions and challenges including the Cyber 9/12 College and Universities competition.

Participants will explore the challenges a country may have when dealing with a national cyber security incident from a non-technical, political, economic social and legal perspective. Participants will also develop their public speaking and presentation skills to discuss cyber security issues at the highest decision-making levels.

The module is intended for school pupils, university and college students and can be adapted to suit the level of learners. (See adaptation section).

Adaptation
The Module has been designed to be suitably adapted and levelled for the learners. The subject matter remains the same but the learning resources can differ for the different learners.

The module has been developed in such a way that teachers, lecturers or trainers can deliver or lead the four sessions as they see fit, depending on their audience. The learning objectives, scenarios, materials and set questions remain the same for all audiences, thus ensuring consistency, but the learning and teaching mode can change as required.

An example of this flexibility would be material normally considered appropriate for third-year PhD students, but not considered suitable for S5 students. This decision must be left to individual teachers who are in the best position to determine the capabilities of the students.

Similarly, the module material includes set questions to use. This ensures consistency. However, instructions are included that module leaders/trainers should ask additional questions based on the presentations. Not only does this allow the module leaders/trainers the flexibility to customise questions according to the aptitudes of the students and the content of their presentation, it also creates a realistic simulation of high-level policy-making and decision-making which can promote the development and practice of public speaking, debating and presenting.

To offer flexible learning, the materials can be used flexibly and students can select additional material made available.

Finally, a digital **Certificate of Completion** can be awarded to all students who complete the module to the satisfaction of Module Leaders. At this stage, the Certificate will not be credit-bearing, but this option may be considered at a later date as the module uptake develops.

Module Aims:

1. To increase understanding of the political, economic, societal, technological, legal and environmental (PESTLE) considerations of a national cyber security incident, recognising the importance of broader, non-technical impacts of cyber security risk.
2. To develop soft skills such as communication and presentation skills which are critical additional skills for the future cyber security workplace.

Module Structure:

The module will be structured around four units. Each unit will comprise of:

- Activities undertaken in **students' own time**:
  - Watching a pre-recorded video micro lecture
  - Undertaking additional reading
- Activities undertaken **with support from the module leader (school/college educator)**:
  - Delivering an oral presentation to the group addressing the weekly learning outcomes and aims.

In total (self-learning and supported learning) the units should require 2-3hrs work per week.

Module Topics:

Over the course of four weeks, students will explore different aspects and impacts of **the Stuxnet incident of 2007**. Stuxnet was chosen due to the wide-ranging and long-term political, economic, societal, technical, legal and (international) strategic impacts of a cyber operation targeting a sovereign state's critical energy infrastructure. There is also a wealth of technical, political, academic and legal analysis in the public domain which students and Module Leaders can draw on if appropriate.

Curriculum

Week 1	Explaining the Technical Challenges
Week 2	Beyond the Middle East: The International Relations impacts of cyber incidents
Week 3	"An attack, or not an attack: that is the question": Cyber Incidents and international law
Week 4	Bringing it all together: Cyber Resilience Policy Development

Week 1: Explaining the Technical Challenges

Students will examine the technical aspects of a major cyber security incident with international consequences. Stuxnet is the example being analysed. The objectives are to

- a) to learn about the technical elements of Stuxnet;
- b) learn about and understand how Stuxnet was deployed and the implications of this for national infrastructure;
- and c) allow students to practise describing and explaining these technical elements to a non-technical audience of decision-makers.

Week 2: Beyond the Middle East: The International Relations' impacts of cyber incidents

Students will examine the international impacts and consequences of major cyber incidents, using Stuxnet as an example. The objectives are to

- a) introduce the concepts and theories of the field of "international relations";
- b) place cyber incidents in that international context, understanding that technological events can have non-technological consequences beyond their immediate vicinity;
- c) enable students to explain and discuss the international implications of cyber incidents to a non-technical or non-IR-expert group of policy-makers

Week 3: "An attack, or not an attack: that is the question": Cyber Incidents and international law

Students will be introduced to the Laws of Armed Conflict (LOAC) and International Humanitarian Law (IHL). These are vast topics, even setting aside the challenges of relating cyber security issues and incidents to these bodies of law. The objectives therefore are to

- a) introduce students to LOAC and IHL, and set out basic foundations for these bodies of law to increase awareness of these legal instruments.
- b) introduce students to the complex nature relationship cyber security and resilience has with IHL and LOAC by examining a major cyber incident (Stuxnet) the legal position of which experts are still discussing
- c) enable students to discuss and explain with increased confidence how cyber incidents relate to international law, acknowledging the complex nature of that relationship and the fact that the students are not trained lawyers.

Week 4: Bringing it all together: Cyber Resilience Policy Development

In the final week of the Module students will bring together the previous three sessions learning to develop holistic policy solutions. The objectives are

- a) for students to understand and be aware of how technology, law and (inter)national politics interact
- b) for students to begin to be able to analyse a major cyber incident from a holistic, non-technical perspective
- c) for students to confidently provide, recommend and discuss holistic cyber resilience policy solutions which do not solely rely on technical tools
- d) for students to navigate the complexities of reserved (Westminster) and devolved (Holyrood) areas of policy in relation to cyber issues.

Commented [CA2]: Incl. the recognition of the challenge Scotland faces as having reserved and devolved.

Commented [RD3R2]: good point

Developing Soft Skills

Recent iterations of the Scottish Cyber 9/12 Strategy Challenge have identified that students, may benefit from support and guidance in developing "soft-skills" – presentation, public-speaking and debating – and also to ensure that technical matters can be presented and explained to non-technical decision-makers such as heads of government.
To facilitate this, there is an assessment and activity plan designed to prepare students to take part in simulation exercises and international competitions, such as the Scottish iteration of the Atlantic Council's Cyber 9/12 Strategy Challenge.

Participation in these external events is completely voluntary, however they provide ideal opportunities to practise these soft skills and present knowledge to non-technical knowledge, but in a **simulated environment**.

Module Resources:

- Weekly micro lectures (10minutes max) recorded by Dr Robert Dewar (Director and Founder, DCC)
- Primer documents on the weekly core topics for S5/S6 school students.
- Academic and industry articles and publications collated by the module designers.
  - NB: While the module designers have made every effort to include open-source material, certain of the academic articles may require institutional logins to access.
- Relevant and moderated YouTube/online videos such as TED talks
- Presentation guidelines for weekly assessments
- Pre-set questions for presentations
- Instructions for student groups on how to divide up team roles
- Instructions for Module Leaders (schoolteachers, college/university staff) on how to interrogate the presentations
- Information and guidance on public-speaking, presentation skills and debate
- Links and primers to NCSC school activities and the Scottish Cyber 9/12 Strategy Challenge where all skills and tools acquired in the module will be put to the test.

Commented [RD4]: These documents are foundational one/two-pagers intended to provide introductions to the complex issues such as IR theory and Stuxnet itself. They are designed to provide summaries while not delving too deep. The objective is not to condescend to the school students but to recognise that this module is completely extra-curricular and students may not have the time to engage effectively with the real-life reports and academic publications also available in the module.

Module Access:

The module will be made available online on the Digliearn website. If the module is hosted on a non-DCC website DCC will make the content available to web-managers in the necessary templates.

All participant resources will be open-source and freely available in the public domain under a “Freeware” principle – all videos recorded by DCC will be copyrighted to DCC but made available for the purposes of this module.

Reading material will also be open source to ensure there are no access issues and to ensure that as many users as possible are able to participate. To ensure copyright for published sources, links to advanced academic resources will be to the document publishers. **This may lead to an access impact for school students and private sector, but uni/college students should be able to use academic institution credentials. Where such logins are required this will be flagged up to users. Alternative open-access materials will be made available.**

Module Learning Outcomes:

1	To determine the non-technical impacts of cyber security
2	To critically evaluate policy, economic, societal, technological, legal, environmental and international relations issues arising from cyber security issues
3	To acquire tools and techniques for discussing, debating and presenting non-technical issues to high-level decision-makers.

Assessment

Formative assessment: *(e.g. quizzes, peer reviewed discussions, case studies with model answers)*
Oral presentations in weeks 1, 2, and 3 moderated and assessed by module leaders/trainers
Summative assessment: (*e.g Graded Assessments, throughout and/or final in week 8)*
In week 4 participants will present a fourth and final team presentation bringing together the findings and details of Weeks 1, 2 and 3

Weekly content breakdown

WEEK 1: Explaining The Technical Challenges of a Major Cyber Incident

Summary of topic covered:

Proposed text for webpage:

In this unit, module participants will delve into the intricate technical dimensions of Stuxnet, an unprecedented cyber weapon, in order to be able to clearly explain technical cyber issues to a non-technical audience of decisionmakers. Exploring its architecture, students will dissect Stuxnet's code, uncovering advanced techniques like code injection and zero-day exploits.

Through videos and real-life technical analyses of a major cyber incident, learners will grasp the malware's propagation methods and its tailored attack on industrial systems, particularly Iran's nuclear facilities. Discussions should revolve around Stuxnet's implications for global cybersecurity, emphasizing the significance of understanding such sophisticated threats. By immersing themselves in Stuxnet's technical intricacies, students will gain insights into the evolving landscape of cyber warfare and the importance of robust defense strategies, while also gaining and practising key discussion skills.

Your Module Leader will divide you into teams of 3-4 for the activities for this week.

Presentation Questions

1. What was the primary attack vector for Stuxnet deployment? What is the significance of this?
2. Which vulnerabilities did Stuxnet exploit?
3. How can a country like Scotland guard against this particular kind of deployment?

Materials

- Micro lecture – Dr R Dewar
- Stuxnet 101 primer document (aimed at S5/S6 students)
- Symantec Stuxnet Dossier
- Stuxnet Facts Report from the NATO Cyber Defence Centre of Excellence, Tallinn, Estonia
- TED talk from Ralph Lagner, cyber security analyst who decoded Stuxnet

Weekly or Unit outcomes (WO)(UO) By the end of this week the student will be able to:	**Activity**	**Brief description of lessons and activities:**
1. Summarise the key events of a cyber incident using Stuxnet as an example	*Watch*	Microlecture from Dr Robert Dewar
	Read Chapter, Page, etc	• Stuxnet 101 primer document (aimed at S5/S6 students) • Symantec Stuxnet Dossier • Stuxnet Facts Report from the NATO Cyber Defence Centre of Excellence, Tallinn, Estonia

Commented [R5]: For Digilearn add in media type (PDF, MP4 etc.)

Commented [R6]: Embedded video

2. Describe to a non-technical audience how a piece of malware was able to enter a secure infrastructure facility
3. Summarise for a non-technical audience how a piece of sophisticated malware operates, using Stuxnet as an example

Watch	TED talk from Ralph Langner		
Discuss	In your teams, examine how Stuxnet operates and its technical impact		
Do	In your groups, prepare a 10minute presentation addressing the unit's three questions: 1. What was the primary attack vector for Stuxnet deployment? What is the significance of this? 2. Which vulnerabilities did Stuxnet exploit? 3. How can a country like Scotland guard against this particular kind of deployment? Be prepared for additional questions from your Module Leader.		
Assessment	10 minute oral presentation and feedback from module leader		

WEEK 2: Beyond the Middle East: The International Relations impacts of cyber incidents

Summary of topic covered:

In this unit, participants will explore how cyber operations and incidents can impact how states interact with one another. Major incidents such as Stuxnet have important geopolitical and geostrategic implications and can change the way states deal with one another.

To understand how cyber operations fit into this complex landscape, participants will first be introduced to the foundations of the field of International Relations. Participants will explore some of the key theories of the field and what they mean, and also examine how "cyber" is changing those theories. The goal is to look beyond purely technical consequences of major cyber incidents and to explore how an incident identified in one part of the world can send political ripples all around the globe.

Finally, participants will look at how private companies engage in international powerplay and what impact this has on international relations and strategy.

1. What was the impact on the international community of:
    a. The discovery of Stuxnet in the open Internet?
    b. The Stuxnet operation itself?
2. Who were the primary players in this operation? What is your evidence/explanation for this?
3. What, if any, was the impact on International Relations of a private company – and not a national security or intelligence agency – discovering and publishing the existence of Stuxnet?

Materials

- Microlecture 1 on International Relations Theories – Dr R Dewar
- Microlecture 2 on International Relations and Cyber security
- Microlecture/YouTube Video Prof Noah Zerbe
- S5/S6 primer on International Relations (IR)
- S5/S6 Primer on cyber security and IR
- Baezner and Robin, Stuxnet Analysis, ETH Zurich
- Vytautas Butrimas, *National Security and International Policy Challenges in a Post Stuxnet World*, 2014, Lithuanian Annual Strategic Review

Weekly or Unit outcomes (WO)(UO) By the end of this week the student will be able to:	**Activity**	**Brief description of lessons and activities:**		
1. Explain the fundamentals of international relations to a non-expert audience	*Watch*	Microlecture on IR and cyber from Dr R Dewar		
	Read Chapter, Page, etc:	• S5/S6 primer on International Relations (IR) • S5/S6 Primer on cyber security and IR • Baezner and Robin, *Stuxnet Analysis*, ETH Zurich • Vytautas Butrimas, *National Security and International Policy Challenges in a Post Stuxnet World*, 2014, Lithuanian Annual		

2. Understand the impact of cyber incidents on international politics. 3. Explain how cyber operations can influence state foreign policy developments.		Strategic Review (academic login may be required)		
	Watch	Prof Noah Zerbe, Humboldt State University https://www.youtube.com/watch?v=h2yiDjqsqqI This video Is heavily focussed on US policy and responses, as that is the topic of the microlecture. However, the overall themes are universal – all states deal with these issues. Prof Zerbe provides an example of how a state responds.		
	Discuss	In your groups, discuss how major cyber incidents such as Stuxnet have an impact on the way states interact with one another.		
	Do	In your groups, prepare a 10minute oral presentation explaining the impacts of major cyber incidents on international politics. Prepare answers to the unit's three questions. 1. What was the impact on the international community of: a. The discovery of Stuxnet in the open Internet? b. The Stuxnet operation itself? 2. Who were the primary players in this operation? What is your evidence/explanation for this? 3. What, if any, was the impact on International Relations of a private company – and not a national security or intelligence agency – discovering and publishing the existence of Stuxnet? Be prepared for additional questions from your Module Leader.		
	Assessment	10 minute oral presentation and feedback from module leader		

WEEK 3: "An attack, or not an attack: that is the question": Cyber Incidents and international law

Summary of topic covered:

In this unit students will be introduced to one of the most complex areas of cyber security: its relationship with international law, specifically the International Laws of Armed Conflict and International Humanitarian Law.

Many major cyber incidents, such as Stuxnet, do not explicitly, categorically or obviously breach international law. Making a case is problematic and requires careful consideration and argument. In this unit, students will receive an introduction to international law, how it can be applied to major cyber incidents, and what states can do should they experience one.

In all of the above, the key skill participants will gain is arguing for and making a case for a particular view, even when there is no clear-cut right or wrong answer. The key skill is creating and presenting a particular case to decision-makers.

One of the critical areas to be covered in this section is the complex relationship between reserved and devolved responsibilities when responding to cyber incidents. While these policy areas are clearly separated between the UK Government (which retains cyber security policy) and the Scottish Government (which is concerned about the impact of a cyber incident on Scotland and its people), the nature of cyber incidents is such that the distinction between devolved and reserved areas is blurred. How policy- and decision-makers navigate these complexities is increasingly important in today's digitalised world.

Commented [CA7]: A ittle on the differences of reserved and devolved in the UK and how this can impact on national decisions re a cyber incident

Commented [R8R7]: done

Set questions for Week 3:

1. In your opinion, can major cyber incidents breach International Law? Explain your answer using Stuxnet as an example.
2. What elements of International Law are relevant to the discussion of major cyber incidents such as Stuxnet?
3. Who or what policies and enforces the international laws relevant to your answers to Questions 1 and 2?
4. Which policy areas that are devolved to Scotland could be impacted by a cyber incident?

Materials

- Microlecture – Dr R Dewar
- S5/S6 primer on LOAC
- S5/S6 primer on Stuxnet and international law
- Prof M Schmitt, *"Attack" as a term of art in International Law: the cyber operations context (academic login may be required)*
  Jansons Janis, *Was Stuxnet an act of war? (Academic login may be required)*

Weekly Unit outcomes By the end of this week the student will be able to:	**Activity**	**Brief description of lessons and activities:**		
	Watch	Microlecture on Law and cyber by Dr R Dewar		
	Read	• S5/S6 primer on LOAC		

1. Understand and describe the fundamental elements of international law.
2. Discuss the fundamental of international law with a non-legal audience
3. Analyze how international law can be applied to significant cyber incidents.
4. Understand the complexity of reserved vs devolved policy between the UK and Scottish Governments during cyber incidents.

Chapter, Page, etc:	• S5/S6 primer on Stuxnet and international law • Prof M Schmitt, *"Attack" as a term of art in International Law: the cyber operations context (academic login may be required)* • Jansons Janis, *Was Stuxnet an act of war? (Academic login may be required)*		
Discuss	In your groups, discuss how, or if, international law can be applied to cyber incidents.		
Do	In your groups, prepare a 10minute presentation addressing the unit's four questions: 1. In your opinion, can major cyber incidents breach International Law? Explain your answer using Stuxnet as an example. 2. What elements of International Law are relevant to the discussion of major cyber incidents such as Stuxnet? 3. Who or what policies and enforces the international laws relevant to your answers to Questions 1 and 2? 4. Which policy areas that are devolved to Scotland could be impacted by a cyber incident? Be prepared for additional questions from your Module Leader.		
Assessment	10 minute oral presentation and feedback from module leader		

Commented [CA9]: adding in the devolved reserved question

WEEK 4: Bringing it all together – Cyber Resilience Policy Development

Summary of topic covered:

In this final week of the Module, participants will explore how non-technical cyber security considerations form the foundation of national and international policy solutions. Cyber security and cyber resilience cannot be achieved by technical means alone. As weeks 1, 2 and 3 of this Module have shown, there are political, economic, social, legal and increasingly environmental considerations to take into account in addition to the technical (the PESTLE approach to cyber security). Effective policy must, if possible, draw together these elements as they are each important parts of wider solutions.

In this unit, students will explore what makes effective policy in the cyber context when dealing with major cyber incidents targeting critical national infrastructure. Crucial to this is the ability to combine and address different thematic areas and create succinct policy recommendations that still achieve particular goals and make states resilient to cyber incidents.

Set questions for presentations in Week 4:

1. Provide 3 policy recommendations to help Scotland be more resilient against Stuxnet-style operations. Think about:
    a. The way Stuxnet entered the target system.
    b. The impact of the operation if successful.
2. Explain and support your choices.
3. What cross-government (UK and Scotland) policy relationships need to be considered?

Materials

- Microlecture – Dr R Dewar
- S5/S6 primer on government policy
- S5/S6 primer on writing cyber policy
- Government Policy Snapshots. A collection of analyses of national government cyber security strategies conducted by Senior Researchers at ETH Zurich's Centre for Security Studies.
- Dr R Dewar and E. Templeton, The Impact of Regulatory Frameworks on the global Digital Communications Industry, 2020, Geneva Centre for Security Policy.
- Dr R Dewar, *Cyber Resilience and the Scottish Third Sector*, 2023, Scottish Government Policy Report

Cyber Resilient Scotland: strategic framework - gov.scot (www.gov.scot)

Weekly or Unit outcomes (WO)(UO) By the end of this week the student will be able to:	**Activity**	**Brief description of lessons and activities:**		
	Watch	Micro lecture on cyber policy from Dr Robert Dewar		

1. combine, summarize and discuss legal, technical and geostrategic impacts of cyber incidents in a single presentation
2. effectively present recommendations for national and international policy to a non-technical, non-legal audience of decision-makers
3. debate, explain and justify policy recommendations in a clear, confident manner

Read Chapter, Page, etc:	• S5/S6 primer on government policy • S5/S6 primer on writing cyber policy • Government Policy Snapshots. A collection of analyses of national government cyber security strategies conducted by Senior Researchers at ETH Zurich's Centre for Security Studies. • Dr R Dewar and E. Templeton, The Impact of Regulatory Frameworks on the global Digital Communications Industry, 2020, Geneva Centre for Security Policy. • Dr R Dewar, *Cyber Resilience and the Scottish Third Sector*, 2023, Scottish Government Policy Report		
Watch	YouTube video on PESTLE analysis from the Chartered Institute of Personnel and Development https://www.youtube.com/watch?v=GFVKKTwkANY This video shows how to conduct a PESTLE analysis for a company, but the lessons and concepts apply well to developing policy for government		
Discuss	In your groups, discuss how to develop holistic policy solutions incorporating, or at least acknowledging and addressing, the political, economic, social, technical, legal and environmental aspects of cyber security		
Do	In your groups, prepare a 10minute presentation addressing the unit's three questions: 1. Provide 3 policy recommendations to help Scotland be more resilient against Stuxnet-style operations. Think about: a. The way Stuxnet entered the target system. b. The impact of the operation if successful.		

	2. Explain and support your choices. 3. Set out the cross-government (UK and Scotland) policy relationships that need to be considered? Be prepared for additional questions from your Module Leader.		
Assessment	10 minute oral presentation and feedback from module leader		

Video transcripts

Week 1 Lecture 1: The Story of Stuxnet: The Cyber Weapon that Changed Everything

Introduction (1 minute)

Welcome, everyone. My name is Dr Robert Dewar and today, I'm going to take you on a journey through the fascinating and complex world of cyber warfare. Our focus will be on a notorious piece of malware called Stuxnet. This cyber weapon, discovered in 2010, has not only changed the landscape of cybersecurity but also international relations and military strategies. Let's dive in and uncover the story of Stuxnet.

Background (2 minutes)

To understand Stuxnet, we first need to grasp the context in which it was developed. This is where studies of the international relations and political machinations between states begins

In the early 2000s, concerns in the West about Iran's nuclear program were escalating. The international community, particularly the United States and Israel, were worried that Iran was developing nuclear weapons under the guise of a civilian nuclear program. Currently, states around the world are legally able to use nuclear power and energy for civilian purposes. That means producing electricity in nuclear power stations or for research in universities, for instance.

What states are not permitted to do – due to a complex series of treaties which we will explore in other sessions – is develop nuclear weapons. Now already you can see some difficulties. Where are the lines drawn between civilian and military nuclear development?

Now, when it comes to Iran's nuclear programme and the West trying to minimise its military application, traditional diplomatic and military options were on the table, but they came with significant risks and potential for escalation. No country likes being told what to do by others. Those are the diplomatic issues.

But countries do have the right to self-defence, and there is a debate among lawyers and legal scholars around whether a pre-emptive strike – like destroying a suspected nuclear weapons facility – is permissible under international law. This is a big debate and there is no clear answer to that question yet.

Enter cyber. Unlike conventional weapons, cyber weapons tools can be deployed discreetly and can potentially cause significant damage to a target without all the messiness of death and destruction. This is where Stuxnet comes into play.

What is Stuxnet? (2 minutes)

Stuxnet is a sophisticated computer worm, a type of malicious software designed to replicate itself and spread to other computers. However, Stuxnet was not your average malware. It was incredibly complex and targeted very specific systems – the industrial control systems, or ICS, that managed Iran's nuclear centrifuges at the Natanz facility, specifically the SCADA networks – supervisory control and data acquisition – of nuclear enrichment centrifuges.

Now, a bit of nuclear physics is needed here.

To get uranium – a radioactive element – to do anything useful in a nuclear reactor or a nuclear weapon it needs to be prepared in a particular way. This is called enrichment. The way that is done is basically to spin it in special devices called centrifuges. Centrifuges are very delicate and spin at very specific speeds to create the kind of uranium that nuclear physicists need for their work. Any changes in that speed and the centrifuges fail, even break to the point of being destroyed.

The brilliance of Stuxnet lay in its precision in two ways. First, it was designed to remain dormant on most computer systems and only activate under very specific conditions. Specific computer hardware made by a specific manufacturer (Siemens in this case) that did a specific function (managing nuclear enrichment systems) which were only found in very few places in the world – including those found at the Natanz nuclear enrichment facility in Iran. If Stuxnet were in any other system that did not meet any one of those conditions, it did nothing. It just sat there.

The second way Stuxnet acted so precisely was, once activated in a network that ticked all the boxes I just mentioned, Stuxnet would subtly alter the speeds of the centrifuges, causing them to spin out of control and ultimately fail. At the same time however, it fed normal operating readings to monitoring systems, ensuring the sabotage went unnoticed by any human staff members for as long as possible.

This is what happened at Natanz. The centrifuges spun out of alignment and control, failed and many were damaged beyond repair. Technically they were destroyed.

What Stuxnet did was very subtle and very clever, and not a single bomb was dropped or bullet fired.

Discovery and Impact (2 minutes)

Stuxnet was discovered in 2010 by a cybersecurity firm called VirusBlokAda. Initially, it baffled security experts because of its complexity and sophistication. That sophistication meant that Stuxnet could not have been created by hacktivists or citizen hackers. Only a large team of highly trained computer specialists with significant resources could pull this off. Not only that, but a great deal of old-school spy intelligence was needed to write code that targeted only these devices and nothing else. This implied state backing. Governments possibly state militaries were doing this.

Further analysis revealed the worm's purpose and the likely involvement of state actors in its creation, with fingers pointing and allegations towards the United States and Israel, who have never officially confirmed or denied their involvement. Although this is part of the “international relations” discussions around Stuxnet, we’re getting into the realms of espionage.

The impact of Stuxnet was profound, however. It reportedly destroyed about a fifth of Iran's nuclear centrifuges and set back their nuclear program by years. But beyond the immediate damage, Stuxnet's discovery sent shockwaves through the cybersecurity community and the world at large. It was the first known instance of a cyber weapon designed to cause physical destruction in a specific manner. This revelation highlighted the potential for cyber attacks to cause real-world damage, changing how nations think about cybersecurity and cyber warfare.

Lessons Learned (2 minutes)

Stuxnet taught us several critical lessons:

1. Cybersecurity Vulnerabilities: Even highly secure, air-gapped systems (isolated from the internet) are vulnerable to cyber attacks. Stuxnet spread through USB drives, showing that even physical barriers can be circumvented.

2. Cyber Warfare Reality: Stuxnet proved that cyber warfare is not just theoretical but a practical tool of modern conflict. It can achieve strategic objectives without the collateral damage associated with conventional warfare.

3. Need for Robust Defence: The sophistication of Stuxnet underscored the need for advanced and multi-layered cybersecurity defences. Organizations and nations must continually evolve their defences to keep up with the ever-changing threat landscape.

4. Ethical and Legal Considerations: Stuxnet raised important ethical and legal questions about the use of cyber weapons. The potential for unintended consequences and collateral damage is significant, and the lack of clear international norms and regulations around cyber warfare is a major concern.

Conclusion (1 minute)

In conclusion, Stuxnet was a game-changer in the world of cybersecurity and international relations. It demonstrated the power and potential of cyber weapons, highlighting both the opportunities and risks they present.

As we continue to advance technologically, and this includes the cyber criminals who are often more than not many steps ahead in terms of their own technological capabilities, the lessons of Stuxnet remain ever-relevant, reminding us of the importance of vigilance, innovation, and ethical considerations in the digital age.

Thank you for joining me in this microlecture on Stuxnet. I hope you found it enlightening and thought-provoking.

See you next time.

Week 2 lecture 1: The International Relations Impacts of Cyber Incidents: Lessons from Stuxnet

Introduction (1 minute)

Hello, everyone. In this session, we are delving into the fascinating world of international relations and cybersecurity, focusing on the profound impacts cyber incidents have on the way countries interact with one another. Our spotlight will be on Stuxnet, a cyber weapon that not only reshaped cybersecurity but also had significant implications for international relations. Let's explore how this piece of malware altered the geopolitical landscape.

Understanding Stuxnet (2 minutes)

To appreciate the international ramifications, we need to first understand what Stuxnet was. Discovered in 2010, Stuxnet was a sophisticated computer worm targeting Iran's nuclear enrichment facilities at Natanz. It was designed to sabotage the facility's nuclear enrichment centrifuges, causing them to malfunction while feeding false data to monitoring systems. The stealth and precision of Stuxnet pointed to a level of expertise and resources suggesting state sponsorship, widely attributed, allegedly, to the United States and Israel.

Diplomatic Implications (2 minutes)

Stuxnet had immediate and far-reaching diplomatic consequences. It marked a shift in how states could pursue their strategic goals. Traditionally, nations resorted to diplomacy, economic sanctions, or military intervention to address security threats. Stuxnet introduced a new tool in the form of cyber warfare, allowing states to achieve significant objectives without any direct confrontation.

There are two specific areas where Stuxnet had an impact.

1. **State Sovereignty and Cyber Espionage**: Stuxnet blurred the lines of state sovereignty. Cyber operations can cross borders invisibly, challenging traditional notions of national boundaries. This raises questions about the extent to which states can defend themselves in cyberspace and what constitutes an act of war when its territory is violated.
2. **Deterrence and Retaliation**: The use of Stuxnet set a precedent for cyber deterrence. Nations now consider cyber capabilities as part of their strategic arsenal alongside conventional weapons – things that go bang. However, the lack of clear norms around retaliation complicates responses. If a state is attacked in cyberspace, what are the appropriate countermeasures? There are laws which speak to responses, but applying those laws is tricky when dealing with cyber weapons. This complexity can escalate tensions, as states may overreact or misinterpret cyber activities.

Impact on International Law and Norms (2 minutes)

As I mentioned, Stuxnet exposed gaps in international law regarding cyber warfare. Traditional international laws, like the Geneva Conventions and the Hague Conventions, do not clearly apply to cyber operations, creating a legal grey area with two key challenges.

1. **Developing Norms and Treaties that states can sign**: In the aftermath of Stuxnet, there have been calls for developing international norms and specific treaties to govern state behavio8r in cyberspace. Efforts such as the United Nations Group of Governmental Experts (UN GGE) have sought to establish some ground rules, but consensus is challenging due to differing national interests and the covert and deniable nature of cyber capabilities.
2. **Attribution and Accountability**: One of the critical issues in cyber incidents is attribution – determining who is behind an attack. Stuxnet highlighted the complexity of attribution, as the responsible parties were not officially confirmed. This complicates holding states accountable and deterring future attacks.

Impact on Global Cybersecurity Posture (2 minutes)

The discovery of Stuxnet also had an effect on global cybersecurity practices. It underscored the need for robust cybersecurity measures across all sectors, not just in critical infrastructure. In particular,

1. **National Cybersecurity Strategies**: Many countries have since developed comprehensive cybersecurity strategies, focusing on protecting critical infrastructure, investing in cyber defenses, and enhancing international cooperation.
2. **Private Sector Involvement**: Stuxnet also highlighted the role of the private sector in cybersecurity. Companies that develop and maintain the digital infrastructure are now key players in national security. Public-private partnerships have become essential in defending against cyber threats.

Ethical and Humanitarian Concerns (2 minutes)

Stuxnet also raised significant ethical and humanitarian concerns in how states interact. The potential for cyber weapons to cause physical harm and disrupt civilian life is a stark reminder of the double-edged nature of technology today.

There is the risk of Collateral Damage when using cyber weapons and tools: Cyber incidents like Stuxnet can have unintended consequences, affecting systems beyond their intended targets. This raises ethical questions about the use of such weapons and the potential harm to innocent civilians who are protected under international law and the laws of war.

This connects to Human Rights: The use of cyber weapons can also impinge on human rights, such as privacy and freedom of information. Balancing national security

with protecting individual rights is an ongoing challenge for everyone in the digital age, but especially for those states seeking to use digital technology for strategic purposes.

Conclusion (1 minute)

In conclusion, Stuxnet was a watershed moment in the realm of international relations and cybersecurity. It demonstrated the strategic value of cyber operations while highlighting significant diplomatic, legal, and ethical challenges. As nations continue to navigate the complex landscape of cyberspace, the lessons from Stuxnet remain crucial. We must strive for international cooperation, robust cybersecurity defences, and prioritise ethical considerations to ensure a secure and stable digital world.

One thing to remember though, is that different governments in different countries will have different ways of doing things, with vastly different reasons for doing so. Not only does this refer to the big players in this, the US, China, Russia…but also much smaller states. Stay tuned for a second micro lecture from me, looking at how Scotland in particular responds to cyber incidents.

For now, thank you for joining me in this exploration of the international relations impacts of cyber incidents through the lens of Stuxnet. I look forward to your questions and further discussion.

Week 2 Lecture 2: Governments and cyber security

Introduction

Hello, everyone. In this microlecture, we're going to explore how governments handle national cyber security incidents. As with the other elements of this unique module, there will be a particular focus on non-technical aspects. Using Scotland as our example, we'll delve into the processes, structures, and roles involved in managing a significant cyber event, particularly in the public sector. We'll also discuss a real-world case involving the Scottish Environment Protection Agency (SEPA) to understand the lessons learned.

1. Detection and Notification

First, detection and notification.

When a national cyber security incident occurs, the detection and notification process is crucial. Typically, a public sector organisation might detect unusual activities through their internal monitoring systems. These could include signs of data breaches, ransomware operations, or other cyber threats.

In the case of SEPA, that organisation identified a ransomware incident when they observed their systems being encrypted and ransom demands being made. Once detected, the first step is to notify the relevant authorities.

2. Initial Notification to Government

The notification process often starts with the affected organisation informing their internal IT and security teams. In Scotland, if it is serious, the affected organisation escalates this by using the Scottish public sector incident notification process and sending notifications to the Scottish Cyber Coordination Centre (the SC3). The SC3 is responsible for national incident response coordination and will bring in other bodies such as the UK's National Cyber Security Centre (NCSC) and Police Scotland as and when appropriate.

At the time of the SEPA incident, however, the SC3 had not yet been established. Instead, at the time, SEPA notified the NCSC directly. The NCSC acts as a central point for cyber incidents in the UK as a whole, not just Scotland, providing support and guidance to manage the threat. SEPA, for instance, reported the incident to the NCSC, which then coordinated the initial response efforts, bringing in the Scottish Government and Police Scotland early on.

This is an important point to make: in a serious cyber incident, rarely does one organisation or institution handle it. Cooperation with other agencies and entities is crucial and necessary. Which brings me to the third key facet of cyber incident response…multi-agency co-ordination.

3. Multi-Agency Coordination

Effective incident management requires coordination across multiple agencies. In Scotland, once notified, the Scottish Government activates its multi-agency response framework. Key players in this framework include:

- The Scottish Cyber Coordination Centre (SC3) as we have heard about. This organisation generally coordinates the national response
- Police Scotland: They handle the law enforcement aspect, including investigation and potential criminal charges.
- The National Cyber Security Centre (NCSC): Provides technical expertise and support, helping to mitigate the impact of the incident.
- But there is also crucial involvement from Local Authorities and Public Sector Organisations: These entities work together to manage the local impact and ensure public services continue to operate. This is resilience and is absolutely vital to an effective incident response: making sure critical services continue to operate while the investigators investigate.
- Finally a Cyber Incident Response (CIR) company may also be involved: depending on the severity of the incident a CIR company may be brought in to examine the cyber incident and support the victim organisation to strengthen their defences, recover from cyber incidents and deliver a full investigation of the incident along with recommendations on how to prevent it happening again.

During the SEPA incident, all these agencies worked together to contain the incident, assess the damage, and begin recovery efforts.

However, if an incident is particularly serious, the involvement of the highest levels of government is sought. This means government ministers.

4. Ministerial Involvement

In the event of a significant national incident, high-level governmental involvement is essential. In Scotland, ministers who would be involved may include:

- The Cabinet Secretary for Justice and Home Affairs: Overseeing the legal and justice response, including coordination with law enforcement.
- The Cabinet Secretary for Constitution, External Affairs and Culture: Engaging with international partners and addressing any diplomatic implications.
- The Cabinet Secretary for Finance and the Economy: Managing the financial impact and supporting economic resilience.
- The Minister for Business, Trade, Tourism and Enterprise: Ensuring the business community is supported and economic activities are safeguarded.
    - All these ministers would be briefed regularly and involved in decision-making to ensure a cohesive response.
- The First Minister and the Deputy First Minister of Scotland would be kept abreast of the incident and notified of any escalation through regular briefings.

5. Role of the National Cyber Security Centre (NCSC)

The NCSC plays a pivotal role in responding to cyber incidents. Their responsibilities include:

- Incident Response: Providing technical assistance to contain and mitigate the incident.
- Threat Analysis: Assessing the nature and scope of the cyber threat.
- Public Communication: Issuing public statements and guidance to inform and crucially reassure the public.
- Recovery Support: Helping organizations recover from the incident and restore normal operations.
- For SEPA, the NCSC's involvement was critical in understanding the incident, advising on response strategies, and supporting recovery efforts.

There is one very important point to remember, however, about the relationship between the NCSC, cyber incidents and Scotland. The NCSC is a United Kingdom agency, which handles responses to incidents across England, Scotland, Wales and Northern Ireland. SEPA is a uniquely Scottish agency. The point here is to remember that there are certain areas of policy – education, the environment, healthcare and housing among others – over which the Scottish Government has jurisdiction. These are "devolved powers" in current jargon.

There are other policy areas, however – such as employment law, foreign affairs, data protection and defence – which remain the responsibility of the Westminster, UK government. These are "reserved powers".

While this may seem overly political, it is important to note the differences in devolved and reserved powers because cyber incidents, and the tools used to carry out those incidents, pay no attention to such idiosyncrasies and have a tendency to leak. They don't stay in one geographical area or remain restricted to one societal infrastructure. The 2017 WannaCry incident, for example, didn't target a particular sector, but the UK NHS and car industry – two very different sectors – were both impacted by it.

This means that policy officials from both the Scottish and UK governments need to establish positive working relationships in order to work together if there is a national cyber incident in any one, several or all of the home nations.

6. Lessons Learned from the SEPA Incident

So, what are the lessons learned from the SEPA incident. Well, it provided valuable insights into managing national cyber incidents in four specific ways:

- First, Preparedness and Resilience: It Emphasised the importance of robust cyber resilience plans and regular training for staff.
- Second, Communication: SEPA Highlighted the need for clear communication channels within and between organizations to ensure timely and accurate information flow.
- Third, Collaboration: The incident Demonstrated the necessity for multi-agency collaboration and the benefits of having predefined roles and responsibilities.
- Fourth and finally, Public Trust: It Reinforced the importance of maintaining public trust through transparency and effective communication during and after the incident.

Conclusion

In conclusion, Managing a national cyber security incident involves a coordinated effort across various government agencies, supported by technical expertise from bodies like the SC£ and the NCSC. The SEPA case exemplifies the importance of preparedness, collaboration, and effective communication in mitigating the impact of such incidents. As cyber threats continue to evolve, these lessons are crucial for enhancing national cyber resilience.

Thank you for watching: see you online.

Week 3 lecture 1 "An Attack, or Not an Attack? That is the Question": Cyber Incidents and International Law

Welcome to this microlecture on one of the most complex and intriguing areas of cyber security: its relationship with international law. Today, we will delve into how international laws of armed conflict and international humanitarian law apply to cyber incidents. We'll discuss how to navigate the ambiguities and complexities of these laws, using major cyber incidents like Stuxnet as a reference. By the end of this lecture, you'll understand the challenges in making a legal case for or against considering a cyber incident as an attack and the importance of developing skills in argumentation and policy navigation.

Introduction to International Law and Cyber Incidents

International law, particularly the laws of armed conflict and international humanitarian law, provides a framework for determining the legality of state actions during conflicts. However, applying these laws to cyber incidents presents unique challenges. Unlike traditional warfare, cyber operations often lack clear, physical manifestations and are shrouded in ambiguity. For example, the Stuxnet worm, which targeted Iran's nuclear facilities and caused enrichment centrifuges to spin out of control, raised significant questions about whether it constituted an act of war or a violation of international law.

Stuxnet: A Legal Case Study

Stuxnet is a prime example of the complexities involved in classifying cyber incidents under international law. While it achieved its intended effect, sabotaging Iran's nuclear program, it did so without causing immediate physical destruction or loss of life. This raises the question: Does Stuxnet qualify as an armed attack under international law?

To answer this, we must consider the criteria for an armed attack. According to the United Nations Charter, an armed attack involves significant force, typically leading to death, injury, or destruction. Stuxnet, however, caused operational disruption without direct physical damage, although it could be argued that physical damage was caused by the worm rendering nuclear enrichment centrifuges useless. This ambiguity highlights the difficulty in applying traditional definitions to cyber incidents.

International Laws of Armed Conflict and Humanitarian Law

The International Laws of Armed Conflict (LOAC) and International Humanitarian Law (IHL) are designed to regulate the conduct of hostilities and protect those not participating in the conflict. These laws emphasize principles such as distinction, proportionality, and necessity. Weapons of mass destruction often fail these tests, because it is almost impossible to distinguish between soldiers and civilians if you are using chemical or nuclear weapons, often the use of such weapons is not proportionate to their military advantage and they are not always necessary – other, smaller weapons could achieve the same effect.

In the cyber realm, applying these principles becomes challenging:

1. **Distinction**: Differentiating between military targets and civilian infrastructure is difficult in cyberspace, where systems are often interconnected, and use the same infrastructure, often down to the same cables.
2. **Proportionality**: Ensuring that the response to a cyber incident is proportionate to the harm caused requires careful assessment of the original incident's impact and often you don't have the time to do that in a conflict.
3. **Necessity**: Justifying a cyber operation based on military necessity involves evaluating whether the action is essential for achieving a legitimate military objective.

Making the Case: Arguing Legal Positions

Given the complexities, making a case for or against classifying a cyber incident as an armed attack requires nuanced argumentation. Legal practitioners and policy-makers must gather evidence, interpret existing laws, and present their arguments convincingly to decision-makers.

For instance, in arguing that a cyber incident like Stuxnet constitutes an armed attack, one might emphasize the strategic impact on national security and the intentional disruption of critical infrastructure. Conversely, opposing arguments might highlight the lack of direct physical harm and the non-traditional nature of cyber operations.

Navigating Reserved and Devolved Policy Areas

Let's add in the complexities of devolved and reserved powers we looked at in the previous session. In the context of the United Kingdom, responding to cyber incidents involves navigating the complexities of reserved and devolved policy areas. Reserved powers are those held by the UK government in London, such as national defense and foreign affairs, while devolved powers are those delegated to regional governments, such as in Scotland, which include areas like education and health.

Cyber incidents often blur these distinctions, as they can impact both national security (a reserved matter) and regional infrastructure (a devolved matter). For example, a cyber attack on Scotland's health services could have national security implications, requiring coordinated responses from both Edinburgh and London.

Policy- and decision-makers must navigate these blurred lines effectively. This involves clear communication, cooperation, and the ability to argue for the necessary allocation of responsibilities and resources. Understanding the interplay between reserved and devolved powers is crucial for developing cohesive and effective cyber resilience strategies.

Conclusion

In conclusion, the relationship between cyber incidents and international law is complex and often ambiguous. By examining cases like Stuxnet and understanding the

principles of international law – proportionality, distinction, necessity – we can begin to navigate these complexities. Developing skills in argumentation and policy navigation is essential for making informed decisions and presenting compelling cases to decision-makers.

As you continue your studies, remember that there are often no clear-cut answers, and the ability to argue effectively and navigate policy complexities is crucial in the ever-evolving field of cyber security.

Thank you for watching, and I look forward to our discussions on this fascinating and challenging topic.

Week 4 lecture 1: Bringing it all together - Cyber Resilience Policy Development

Welcome to this microlecture on cyber resilience policy development. Today, we'll explore how non-technical considerations form the foundation of national and international policy solutions.

As we've seen in the first three weeks of this module, achieving cyber security and resilience involves more than just technical measures. Political, economic, social, legal, technological and environmental factors—the PESTLE approach—are all crucial in creating effective policies. Let's delve into these considerations and understand how they shape policies that safeguard critical national infrastructure from major cyber incidents.

Introduction

Cyber resilience is the ability to prepare for, respond to, and recover from cyber incidents. This concept goes beyond traditional cyber security, which focuses mainly on preventing incidents taking place. Effective cyber resilience requires a holistic approach that integrates various non-technical aspects. By examining the cases of Scotland's cyber resilience strategy and the Stuxnet incident, we can see how these considerations come into play.

Technical considerations for cyber resilience are well-covered: having effective anti-virus software, using multifactor authentication, those sorts of measures. But what about the other parts of PESTLE?

Political Considerations

Let’s start with political considerations.

Political factors are vital in shaping cyber resilience policies. National strategies must prioritize the protection of critical infrastructure from cyber threats. Governments need to foster international cooperation, forming alliances and agreements to combat cyber threats that transcend borders. For instance, Scotland's cyber resilience strategy

emphasizes collaboration across government, industry, and academia to build a secure and resilient digital nation. Political will and leadership are essential in prioritizing and funding cyber security initiatives.

Economic Considerations

Next are economic considerations. Economic factors are pivotal in understanding the impact of cyber threats. Cyber incidents can have devastating economic consequences, disrupting industries and costing billions in damages. Policies must emphasize economic resilience, ensuring that businesses can recover swiftly from incidents. Investment in cyber security infrastructure is crucial. Governments can incentivize private sector investment in cyber security, for instance, through tax breaks or grants. Scotland's approach includes supporting businesses in improving their cyber security measures, recognizing that a resilient economy requires robust defences across all sectors.

Social Considerations

But what about society itself? Cyber security policies must account for the social dimension. Public awareness and education are key components in creating a cyber-resilient society. Social engineering operations exploit human vulnerabilities, and thus, educating citizens about these threats can reduce their impact. Policies should promote digital literacy and foster a culture of security within organizations and communities. Inclusive policies that consider the needs of diverse populations, including the elderly and marginalized groups, can ensure broader societal resilience. Scotland's strategy involves initiatives to raise cyber security awareness among the general public and specific sectors, promoting a culture of vigilance.

Legal Considerations

The legal framework surrounding cyber security is complex and constantly evolving. Effective policies require comprehensive legislation that addresses cybercrime, data protection, and privacy. But laws must be adaptable to the rapid pace of technological change and the emergence of new threats. International legal cooperation is also crucial. Harmonizing laws across countries can facilitate better cooperation in prosecuting cybercriminals and sharing threat intelligence. The Stuxnet incident, which targeted Iran's nuclear facilities, highlights the importance of international legal frameworks. Stuxnet's sophisticated nature and geopolitical implications underscore the need for collaborative legal efforts to address such threats.

Environmental Considerations

And finally, environmental considerations. Although often overlooked, environmental factors are becoming increasingly relevant in cyber security. The environmental impact of cyber infrastructure, such as energy consumption by data centres, is enormous. Policies must promote sustainable practices, ensuring that cyber security measures do not exacerbate environmental issues. Moreover, as climate change increases the

frequency of natural disasters, policies must consider the resilience of cyber infrastructure to such events. Ensuring that data centres and critical systems are protected against environmental threats is essential for maintaining cyber resilience.

Integrating PESTLE in Policy-Making

To create effective cyber resilience policies, it's essential to integrate these PESTLE factors. A multi-faceted approach allows for comprehensive solutions that address the complexity of cyber threats.

Here are some key steps in developing such policies:

1. **Risk Assessment**: Conduct thorough assessments that consider political, economic, social, legal, and environmental risks alongside technical vulnerabilities.
2. **Stakeholder Collaboration**: Engage stakeholders from various sectors, including government, private industry, academia, and civil society, to ensure diverse perspectives and expertise.
3. **Regulatory Frameworks**: Develop adaptable legal frameworks that can respond to evolving threats and foster international cooperation.
4. **Public Awareness**: Implement education campaigns to raise awareness about cyber security threats and promote a culture of vigilance.
5. **Sustainability**: Ensure that cyber security measures are sustainable and consider their environmental impact.
6. **Resilience Planning**: Create contingency plans that account for a wide range of scenarios, including political instability and natural disasters.

A great example of this is Scotland's approach to the ransomware incident which targeted the Scottish Environmental Protection Agency, SEPA. To respond to that incident, a multi-agency approach was taken to ensure that law enforcement, technical experts, ministerial direction and liaison with UK cyber security agencies all collaborated to ensure the impact of the cyber incident was minimised and SEPA's work could continue.

Conclusion

In conclusion, achieving cyber resilience requires more than just technical solutions. By incorporating political, economic, social, legal, technological *and* environmental considerations into policy-making, we can develop comprehensive strategies that enhance national and international resilience to cyber incidents. As you continue your studies in this module, remember that effective cyber resilience policy is an intricate mosaic of these diverse elements, each contributing to a robust and resilient cyber defence posture. By learning from examples like Scotland's comprehensive strategy and the global lessons from Stuxnet, we can craft policies that protect our critical infrastructures and society as a whole.

Thank you for watching. See you online.