I. Introduction

The document entitled "Why major Powers launch destructive cyber operations and what to do about it" by the German Council on Foreign Relations (DGAP) will be carefully analyzed to ensure a comprehensive understanding of the various aspects and nuances of the author's idea.

This analysis will examine the alleged motives behind the initiation of cyber activities by major Powers, the consequences of such actions, and strategic responses that can be formulated to address this growing problem.

The main focus is to analyze past destructive cyber operations to better understand and predict future damaging campaigns, as well as to propose strategies for dealing with such threats.

This analysis aims to provide valuable information for (but not limited to) cyber security professionals and strategic planners

A. Thoughts

The publication is part of DGAP's broader research on technology and its impact on international relations, including the cybersecurity dimensions of smart cities and the risks associated with technological dependencies. It also fits within the context of global security challenges, such as cyber warfare and the spread of weapons of mass destruction, and the need for strategic responses to these threats.

The article provides a comprehensive overview of the positive and negative aspects of cybersecurity. The author highlights the advancements in security technology, such as advanced encryption techniques, biometric authentication, and AI-powered threat detection, as positive aspects. The increased public awareness of cybersecurity issues is also seen as a positive development. On the negative side, the author points out the persistence of threats, the shortage of cyber awareness, and the involvement of criminal organizations.

Criticism of the article could include a lack of depth in discussing the negative aspects of cybersecurity. While the author mentions the persistence of threats and the involvement of criminal organizations, they do not delve into the specifics of these issues or provide concrete examples. Additionally, the article could benefit from a more detailed discussion on potential solutions to these problems.

The relevance of the author's expertise to the article's content is crucial. An author with a background in cybersecurity would have a deep understanding of the field's complexities, enabling them to provide insightful analysis and informed opinions. This expertise would also lend credibility to the article, making it a reliable source of information for readers.

In terms of the article's positive and negative sides, it provides a balanced view of cybersecurity, highlighting both its advancements and ongoing challenges. This comprehensive perspective is beneficial for readers seeking to understand the current state of cybersecurity. However, the article could be improved by providing more detailed information on the negative aspects of cybersecurity and discussing potential solutions to these issues.

II. KEY FINDINGS

The section presents several key points, secondary points, and takeaways.

A. Main & Secondary Points:

The main motivations for launching destructive cyber operations are territorial conquest, threat prevention, and retaliatory actions.

The first known cyber operation that destroyed physical objects was Stuxnet, an American-Israeli operation in 2010 that sabotaged Iranian uranium enrichment centrifuges.

The sample size of destructive great power cyber operations targeting states outside of a major conflict is rather limited. Historically, there have been five series of destructive operations (i.e., cyber campaigns).

All cyber campaigns examined took place in a dichotomy. Power asymmetries were extensive. Great powers, the United States and others, were able to conduct cyber operations as they felt secure and did not fear any major backlash were not afraid of any serious reaction to the actions taken.

B. Key Findings:

Iran, North Korea, South Korea, Ukraine, and Taiwan have been the main targets of destructive cyber operations by great powers.

For the US, future targets will highly likely be limited to countries that aim to acquire nuclear weapons, such as Iran and North Korea, as well as expanding its economic influence in the South Asian region.

Given ongoing border disputes, several countries, particularly China, are likely to target neighboring countries with destructive cyber campaigns.

C. Key Takeaways:

The publication emphasizes the need for a comparative analysis of why hegemons conduct destructive cyber campaigns and provides recommendations for what Germany and other European Union member states can do to mitigate them.

The publication defines destructive cyber operations as those causing death or human injury, considerable physical damage, or significant economic loss.

The publication also highlights the importance of attribution in cyber operations, noting that some operations were excluded from the analysis due to non-definitive attribution claims.

III. A Short History of Destructive Cyber Campaigns

The section provides an overview of significant cyber campaigns that have occurred in the past, focusing on their motivations, impacts, and commonalities.

The first major cyber campaign discussed is the US-Iran conflict from 2010-2019. The Stuxnet operation in 2010, which targeted nuclear enrichment facilities in Natanz, Iran, is a notable example. In 2019, the US disabled Iranian databases used to attack oil tankers in the Gulf.

The US-North Korea conflict from 2014-2017 is another significant campaign. However, the analysis excludes some operations due to non-definitive attribution claims, such as China causing power outages in India in 2021 and shutting down a port in Japan in 2023, and the US causing explosions of a Russian gas pipeline.

The commonality among these campaigns is the motivation to degrade an adversary's attack capabilities. For instance, the US deployed destructive campaigns against North Korea and Iran to delay their acquisition and deployment of offensive weapons.

IV. Commonalities of Past and Next Big Destructive Cyber Campaigns

Destructive cyber campaigns share common motivations, such as degrading an adversary's capabilities, causing significant physical damage, and even causing human injury

Destructive cyber campaigns are often conducted by hegemons to degrade an adversary's attack capabilities.

The use of wipers, a type of malware that destroys data, is a common tactic in these campaigns

These campaigns can cause significant physical damage and even human injury.

Non-definitive attribution claims can make it challenging to include all operations in an analysis of cyber campaigns

The sophistication and expertise of the attackers, the indiscriminate scope of the attacks, and the targeted, hostile intent to maximize damage are common characteristics of these campaigns

The use of artificial intelligence and advanced threat intelligence has improved the detection of these attacks

The attribution of cyber campaigns can be complicated due to the ability of actors to hide their identities, impersonate other computers, use virtual private networks to complicate surveillance, or hijack other devices to undertake operations

The international community has not yet formally established a convention categorizing cyber warfare, but it has taken steps to define it

The growing cyber threat could eventually force a reconsideration of the meaning of weapons of mass destruction

The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by walls and oceans.

The next big destructive cyber campaign could be driven by a variety of motivations, including geopolitical tensions, financial gain, or the desire to cause significant physical damage or human injury

The growing cyber threat could eventually force a reconsideration of the meaning of weapons of mass destruction

The international community has not yet formally established a convention categorizing cyber warfare, but it has taken steps to define it

Cyber attacks have touched 120 countries, fueled by government-sponsored spying and with influence operations (IO) also rising

The scale and nature of threats outlined in the Microsoft Digital Defense Report can appear daunting, but huge strides are being made on the technology front to defeat these attackers

V. What to Do

The section 'What to Do' discusses strategies and recommendations for mitigating the impact of destructive cyber operations

The publication suggests that countries should focus on building their cybersecurity capacity and intelligence gathering, particularly in relation to threats to the financial system

It also emphasizes the importance of international collaboration in combating cyber threats, given the globally interdependent nature of the system

The document highlights the need to reduce fragmentation among stakeholders and initiatives, which currently hampers international cooperation and weakens the system's recovery and response capabilities

The publication mentions that countries need to develop better ways and means for countering cyber-enabled information operations

It also discusses the idea of creating new tools to address the goals that different countries have for the way they operate in cyberspace

The document suggests that the Great Powers should consider how to use cyber operations to bolster deterrence of coercion and armed attack

A. Key Takeaways:

International collaboration is crucial in combating cyber threats, given the globally interdependent nature of the system.

There is a need to reduce fragmentation among stakeholders and initiatives, which currently hampers international cooperation and weakens the system's recovery and response capabilities.

There is a need to create new tools to address the goals that different countries have for the way they operate in cyberspace.