AKTOR DALAM SEKURITISASI PADA ISU *CYBER ATTACK* DI ESTONIA (2021-2023)

(Skripsi)

Oleh

MUHAMMAD BAYU

1716071044

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2024

AKTOR DALAM SEKURITISASI PADA ISU *CYBER ATTACK* DI ESTONIA (2021-2023)

Oleh

MUHAMMAD BAYU

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA HUBUNGAN INTERNASIONAL

Pada

Program Sarjana Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik

JURUSAN HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
2024

ABSTRAK

AKTOR DALAM SEKURITISASI PADA ISU *CYBER ATTACK* DI ESTONIA (2021-2023)

Oleh

MUHAMMAD BAYU

Estonia, merupakan negara yang merdeka dari Uni Soviet, semenjak kemerdekaannya, Estonia mengalami kemajuan dalam tekonologi dan digitalisasi, tetapi di tengah kemajuan, Estonia menghadapi tantangan ancaman yang ditimbulkan dari kemajuan teknologi tersebut, yakni serangan *cyber*. Estonia mendapatkan serangan *cyber* pertama tahun 2007, ini merupakan kilas balik Estonia untuk bangkit melawan ancaman *cyber*. Meskipun Estonia sudah melakukan sekuritisasi terhadap ancaman *cyber* di tahun 2007, namun pada faktanya Estonia masih mendapatkan serangan *cyber* hingga saat ini (2023).

Penelitian ini menganalisis aktor dalam sekuritisasi pada ancaman *cyber* di Estonia di tahun 2021-2023. Pendekatan kualitatif deskriptif konsep sekuritisasi Buzan. Fokus penelitian adalah mengidentifikasi aktor yang terlibat dalam melakukan sekuritisasi pada ancaman *cyber* di Estonia pada tahun 2021-2023. Data sekunder digunakan sebagai pengumpulan data melalui analisis *content analysis* dari studi literatur, situs berita resmi, dokumen jurnal riset, dan situs organisasi terkait. Analisis data peneliti mengadopsi dari teknik Miles dan Huberman tahun 2014.

Hasil penelitian menunjukan, bahwa ancaman *cyber* di Estonia yang terjadi di tahun 2021-2023 masih terus berlanjut. Analisis aktor dalam sekuritisasi pada serangan *cyber* analisis menyoroti *referent object* Estonia sebagai Negara dan anggota NATO, untuk peran *securitizing aktor* Alar karis melalui klaimnya dan melibatkan pemerintah Estonia dan organisasi NATO sebagai aktor *audience* memberikan perhatian pada isu ancaman *cyber* dan Kalle Laanet. identifikasikan sebagai *functional actor* adalah CERT. Penelitian ini untuk memberikan pemahaman pada upaya Estonia dalam menunjukan pentingnya peran aktor sekuritisasi terhadap ancaman *cyber*.

Kata Kunci: Estonia, Aktor Sekuritisasi, Serangan *Cyber*, NATO

ABSTRACT

AKTOR IN THE SECURITIZING OF CYBER ATTACK IN ESTONIA (2021-2023)

By

MUHAMMAD BAYU

Estonia, a country that gained independence from the Soviet Union, has experienced significant technological and digital advancement since its independence. However, amidst these advancements, Estonia faces challenges posed by the very progress in technology, namely cyber attacks. Estonia experienced its first cyber attack in 2007, which served as a wake-up call for Estonia to rise against cyber threats. Despite having securitized against cyber threats in 2007, Estonia continues to face cyber attacks up to the present day (2023). This research analyzes the actors involved in the securitization of cyber threats in Estonia from 2020 to 2023. A qualitative descriptive approach using Buzan's securitization concept is employed. The research focuses on identifying the actors involved in the securitization of cyber threats in Estonia during this period. Secondary data was collected through content analysis of literature studies, official news sites, research journal documents, and related organizational websites. The data analysis technique adopted by the researcher is from Miles and Huberman's 2014 method. The results of the study show that cyber threats in Estonia continued from 2020 to 2023. The analysis of securitization actors in the cyber attacks highlights Estonia as the referent object, both as a state and a NATO member. Securitizing actors such as Alar Karis, through their claims, involve the Estonian government and NATO organizations as audience actors to draw attention to the issue of cyber threats. Kalle Laanet is identified as a functional actor with CERT (Computer Emergency Response Team). This research aims to provide an understanding of Estonia's efforts to highlight the importance of securitizing actors in addressing cyber threats.

Keywords: Estonia, Securitization actor, Cyber attacks, NATO

Judul Skripsi : **AKTOR DALAM SEKURITISASI PADA ISU *CYBER ATTACK* DI ESTONIA (2021-2023)**

Nama Mahasiswa : *Muhammad Bayu*

Nomor Pokok Mahasiswa : **1716071044**

Program Studi : **Hubungan Internasional**

Fakultas : **Ilmu Sosial dan Ilmu Politik**

MENYETUJUI

1. Komisi Pembimbing

Indra Jaya Wiranata, S.IP., M.A.	**Nibras Fadhlillah, S.IP., M.Si.**
NIP 19921219 202203 1 011	NIP 19931203 202203 2 010

2. Ketua Jurusan Hubungan Internasional

Simon Sumanjoyo H, S.A.N., M.PA.

NIP 19810628 200501 1 003

MENGESAHKAN

1. **Tim Penguji**

Ketua : **Indra Jaya Wiranata, S.IP., M.A.**

Sekretaris : **Nibras Fadhlillah, S.IP., M.Si.**

Penguji Utama : **Gita Karisma, S.IP., M.Si.**

2. **Dekan Fakultas Ilmu Sosial dan Ilmu Politik**

Dra. Ida Nurhaidi, M.Si.
NIP. 19610807 198703 2 001

Tanggal Lulus Ujian Skripsi : **12 Juni 2024**

PERNYATAAN

Dengan ini saya menyatakan bahwa

1. Karya tulis saya, skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana), baik di Universitas Lampung maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan komisi pembimbing dan penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan sebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah berlaku di Universitas Lampung.

Bandar Lampung, 10 Juni 2024

Yang membuat pernyataan,

Muhammad Bayu
1716071044

Catatan

Pernyataan ini diletakkan pada halaman setelah abstrak.

RIWAYAT HIDUP

Penulis bernama lengkap Muhammad Bayu lahir di Panjang, Bandar Lampung pada tanggal 14 September 1999, sebagai anak ketiga dari empat bersaudara, dari Bapak Taufik Sosio Andrianto dan Ibu Siti Maemunah, S.Pd.

Untuk riwayat pendidikan penulis menempuh pendidikan taman kanak-kanak (TK) Bina Harapan Panjang, Bandar Lampung diselesaikan pada tahun 2005, pendidikan Sekolah Dasar (SD) Negeri Labuhan Ratu Satu Way Jepara, Lampung Timur diselesaikan pada tahun 2011, lanjut pada tingkat Sekolah Menegah Pertama (SMP) Muhammadiyah 1 Way Jepara, Lampung Timur diselesaikan pada tahun 2014 dan menempuh Sekolah Menebgah Atas (SMA) Negeri 1 Way Jepara, Lampung Timur diselesaikan pada tahun 2017.

Pada tahun 2017 penulis terdaftar sebagai mahasiswa Hubungan Internasional FISIP Unila melalui jalur Seleksi Bersama Masuk Perguruan Tinggi (SBMPTN). Selama menjadi mahasiswa penulis pernah melaksanakan Praktik Kerja Lapangan (PKL) di Dinas Perhubungan provinsi Lampung dan Kesyahbandaran Operasi Pelabuhan periode Januari-Februari 2020, kemudian lanjut pada Oktober 2022-April 2023 melanjutkan *internship* di Dinas Perhubungan provinsi Lampung.

MOTTO

“selama masih mempunyai tekad berjuang saya meyakini, saya tidak kalah dan belum kehilangan, meskipun membutuhkan waktu yang lama serta biaya yang tidak kecil dalam perjuangan. Kesia-siaan muncul ketika berhenti untuk berjuang”

Muhammad Bayu

“J M M”

Lalo Salamanca

PERSEMBAHAN

Ku persembahkan skripsi ini kepada:

Tuhan Yang Maha Esa, Allah Azza Wa Jalla, karena nikmatnya sehingga saya bisa menyelesaikan skripsi ini dengan cukup baik dan semoga melalui skripsi ini bisa menjadi amal ibadah saya kepadanya.

Kepada kedua orang tuaku yaitu bapak Taufik Sosio Andrianto dan ibu Siti Maemunah, S.Pd yang saya amat saya banggakan, semoga skripsi ini bisa menjadi kebanggan ayah dan ibu yang selalu senantiasa sabar dalam membimbing saya.

Kepada saudara-saudara dan saudariku yang selalu menanyakan perihal kelulusan saya.

Dan juga kepada jurusan Hubungan Internasional Universitas Lampung yang saya banggakan.

SANWANCANA

Alhamdulillah puji syukur atas keridhoan Allah SWT yang senantiasa memberi rahmat dan karunia-Nya, peneliti dapat menyelesaikan skripsi ini yang berjudul, "Sekuritisasi terhadap ancaman *cyber* di Estonia terkait serangan *cyber* dari Rusia". Shalawat serta salam selalu tercurahkan kepada Nabi Muhammad SAW. Skripsi ini merupakan salah satu syarat untuk menyelesaikan studi dan memperoleh gelar Sarjana Ilmu Hubungan Internasional pada Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung. Peneliti mendapat bantuan dan dukungan dari berbagai pihak saat menyusun skripsi ini. Pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Allah Azza Wa Jalla atas keridhoannya selama ini dalam hidup saya dan Nabi Muhammad SAW atas syafaatnya kepada umat manusia hingga akhir zaman.
2. Ibu Dra Ida Nurhaida, M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.
3. Bapak Indra Jaya Wiranata, S.IP., M.A., selaku dosen pembimbing utama saya yang membantu, membimbing, dan mengarahkan dalam pengerjaan skripsi ini.

4. Ibu Nibras Fadhlillah, S.IP., M.Si., selaku dosen pembimbing kedua saya yang sudah meluangkan waktu untuk membantu, membimbing, dan mengarahkan dalam pengerjaan skripsi ini.
5. Ibu Gita Karisma, S.IP., M.Si., Selaku dosen pembahas dan penguji yang sudah memberikan kritik dan saran yang sangat berguna bagi penyusunan skripsi saya.
6. Bapak Iwan Sulistyo, S.Sos., M.A., selaku dosen yang pernah membimbing saya yang telah meluangkan waktu untuk membimbing, mengarahkan, serta membantu dalam skripsi saya hingga menyelesaikan skripsi ini.
7. Seluruh jajaran dosen Jurusan Hubungan Internasional Universitas Lampung dan Staf Jurusan atas dukungan pembelajaran selama perkuliahan, serta membantu proses administrasi.
8. Keluarga besar di Pesawaran dan Kalianda yang sudah mendo'akan dan memberi semangat kepada saya.
9. Agung Sarwoko dan Imam merupakan kawan yang selalu memberi nasihat ketika saya mulai merasa putus asa.
10. Seluruh anggota *Break The Limit*, yaitu Cyril Noor, Farid A, Fausta Herlambang, Fauzi Pamungkas, Rodo Arif Sinaga, Vincent Dion P, dan Satria Aji B. kelompok ini luar biasa mereka yang selalu senantiasa ada saat saya membutuhkan pertolongan.
11. Nadira Ramadhia A. terimakasih atas saran dan informasinya semasa saya kuliah juga dalam masa pengerjaan skripsi.

12. Syifa Fauziyyah merupakan wanita luar biasa yang mengingatkan untuk menyerahkan kesulitan dalam skripsi untuk diserahkan pada Allah Azza Wa Jalla.
13. Teman-teman Angkatan 2017 Jurusan Hubungan Internasional Universitas Lampung yang menjadi penyemangat dalam penulisan skripsi ini, semoga kita semua dapat menggapai cita-cita kita masing-masing dan selalu dilindungi Tuhan.
14. Serta seluruh pihak yang telah mendo'akan dan mendukung saya dalam penulisan.

Bandar Lampung

Penulis

Muhammad Bayu

DAFTAR ISI

Halaman

MENYETUJUI **5**

1. Tim Penguji 6
2. Dekan Fakultas Ilmu Sosial dan Ilmu Politik 6

DAFTAR ISI ..... **i**

DAFTAR TABEL ..... **iii**

DAFTAR GAMBAR ..... **iv**

DAFTAR SINGKATAN ..... **v**

I. PENDAHULUAN **2**

1.1 Latar Belakang 2

1.2 Rumusan Masalah 4

1.3 Tujuan 4

1.4 Manfaat 4

1.4.1 Manfaat Teoretis 4

1.4.2 Manfaat Praktis 4

II. TINJAUAN PUSTAKA **5**

2.1 Penelitian Terdahulu 5

2.2 Landasan Teori dan Konsep 9

2.2.1 *Securitization* 10

2.2.2*,*Cyber Attack 16

2.3 Kerangka Pemikiran 16

III. METODE PENELITIAN **18**

3.1 Jenis Penelitian 18

3.2 Fokus Penelitian 18

3.3 Jenis dan Sumber Data 18
3.4 Teknik Pengumpulan Data 19
3.5 Teknik Analisis Data 19
IV. HASIL DAN PEMBAHASAN 21
4.1 Kasus *Cyber Attack* di Estonia 21
4.1.1 Serangan *Cyber* 2007.....21
4.1.2 Kasus *Cyber Attack* (2021-2023).....25
4.2 Analisis Aktor Yang Terlibat Dalam Sekurtisasi di Estonia Terhadap Ancaman *Cyber* (2021-2023).....27
Analisis Aktor Yang Terlibat dalam Sekuritisasi pada Ancaman *Cyber* Di Estonia Pada Masa Kini (2023) 28
V. SIMPULAN DAN SARAN.....46
5.1 Simpulan.....46
5.2 Saran.....47
DAFTAR PUSTAKA.....48

DAFTAR TABEL

Tabel Halaman

Tabel 2.1 Perbandingan penelitian terdahulu.....8
Tabel 4.2 Persentase Penggunaan Bahasa di Estonia 32

DAFTAR GAMBAR

Gambar Halaman

Gambar 2.3 Kerangka Pemikiran 17
Gambar 4.1 Penampakan patung The Bronze Soldier 23

DAFTAR SINGKATAN

CCDCoE	: *Cooperative Cyber Defence Centre of Excellence*
CDP	: *Cyber Defence Pledge*
CERT	: *Computer Emergency Response Team*
CIS	: *Commonwealth of Independent State*
DDoS	: *Distributed Denial of Service*
EDF	: *Estonia Defence Force*
IP	: *Internet Protocol*
IT	: Informasi dan Teknologi
NATO	: *North Atlantic Treaty Organization*
PESCO	: *Permanent Structure Cooperation*
TUT	: *Tallinn University Technology*
UE	: Uni Eropa

I. PENDAHULUAN

1.1 Latar Belakang

Estonia, merupakan sebuah negara baltik yang merdeka dari Uni Soviet. Setelah Merdeka Estonia mengalami transformasi signifikan khususnya dalam hal kemajuan teknologi, tetapi di tengah kemajuan yang dialami, Estonia juga menghadapi tantangan serius dalam keamanan, seperti mengalami serangkaian peristiwa pada serangan *cyber* ditahun 2007 (Kozlowski, 2014). *Cyber attack* telah menjadi ancaman serius dalam dunia modern yang semakin tergantung pada teknologi informasi dan komunikasi. Sebagai salah satu Negara dengan tingkat digitalisasi tertinggi di dunia, Estonia telah menjadi targer pada *cyber* attack, seperti yang dialami tahun 2007. Serangan ini tidak hanya mengganggu infrastruktur digital Negara, tetapi juga menjadi titik balik dalam memandang ancaman *cyber* (Ottis, 2011).

Sejak serangan yang dialami oleh Estonia, hal tersebut menjadi titik balik untuk memperkuat pemahaman, bahwa pentingnya keamanan *cyber* dalam konteks pada kesadaran tentang potensi ancaman yang ditimbulkan oleh serangan *cyber,* seperti ancaman *cyber.* Di era digital yang semakin maju serangan *cyber* pada tahun 2007, Estonia telah meningkatkan upaya untuk keamanan *cyber* dan memahami ancaman serius dari *cyber* sebagai ketahanan kedaulatan. Serangan *cyber attack* terus berlanjut hingga saat ini (2023) masih dihadapi Estonia. Sejak kasus serangan *cyber* sejak tahun 2007, Estonia tetap mendapatkan serangan. Serangan-serangan tersebut bahkan lebih kompleks, seperti penyerangan terhadap rumah sakit di tahun 2021 dan serangan pada Perusahaan pembangkit tenaga listrik nasional di tahun 2022. Serangan yang dilakukan lebih bervariasi. Tidak

hanya serangan DDoS saja yang terjadi, serangan *cyber* bertambah jenisnya, seperti *ransomware* dan *phishing* (Ministry of Defence of Estonia, 2019). Target serangan tetap menargetkan infrastruktur digital yang bernilai vital, seperti stabilitas politik, ekonomi dan sosial. Ini membuktikan meskipun Estonia sudah membuka ruang untuk keamanan *cyber*, akan tetapi Estonia masih tetap terancam pada serangan *cyber*. Serangan ini tidak hanya ditujukan pada sector pemerintahan tetapi juga menargetkan infrastuktur listrik yang mempengaruhi aktivitas missal warga, hal ini menuntun pada pendekatan dalam mengidentifikasi ancaman (Information System Authority, 2021)

Konsep sekuritisasi yang dikembangkan oleh buzzan, menyediakan analitis untuk memahami isu *cyber attack* sebagai konsep dalam teori keamanan, merujuk kepada proses pada suatu isu yang dianggap sebagai ancaman keamanan yang memerlukan respon dari aktor sekuritas dengan tujuan untuk memitigasi ancaman (Barry Buzan, 1998). Dalam konteks isu yang dialami Estonia. Dengan adanya dorongan aktor-aktor yang terkait untuk mengambil langkah serius dalam menghadapi ancaman *cyber* di Estonia. Pada hal ini sangat penting untuk memahami aktor-aktor yang terlibat dalam sekuritisasi terhadap ancaman *cyber* di Estonia. Tujuannya untuk memahami dan menjelaskan upaya yang dilakukan Estonia dalam menghadapi ancaman *cyber* untuk dimasukan dalam konsen keamanan. Selain itu, meski peristiwa serangan *cyber* sudah terjadi lebih dari satu dekade. Kepentingan untuk memahami atas ancaman *cyber* di Estonia masih tinggi.

Penelitian ini memberikan fakta atas aktor-aktor yang terlibat tentang Estonia dalam merespon ancaman *cyber* sebagai bagian dari proses keamanan, serta upaya atau usaha-usaha Estonia untuk memberikan konsen pada ancaman *cyber*. Penelitian ini pula menjabarkan aktor-aktor sekuritisasi Estonia pada ancaman *cyber* di periode 2021-2023 dan upaya-upaya dalam mempertahankan kemanan Estonia dari ancaman *cyber*. Dengan demikian, latar belakang ini untuk memberikan landasan yang kuat dalam penelitian yang lebih lanjut pada aktor yang terlibat dalam sekuritisasi terhadap isu *cyber* di Estonia 2021-2023.

1.2 Rumusan Masalah

Estonia berfokus pada titik untuk konsen dalam memperhatikan keamanan *cyber* hingga saat ini. Untuk memahami Estonia dalam menanggapi atau konsen pada isu ancaman *cyber*, perlu mencermati aktor yang terlibat dalam proses sekuritisasi. Dengan menelusuri aktor kita dapat memahami dinamika yang mempengaruhi masuknya ancaman *cyber* kedalam konsen keamanan Estonia. Oleh karena itu, penelitian ini hendak menjawab satu pertanyaan, yaitu:

"Siapa saja aktor yang terlibat dalam sekuritisasi pada isu *cyber attack* di Estonia 2021-2023?"

1.3 Tujuan

Penelitian ini memiliki dua tujuan, yakni:

1. Mendeskripsikan isu *cyber attack* di Estonia 2021-2023.
2. Menganalisis aktor yang terlibat dalam sekuritisasi terhadap isu ancaman *cyber* di Estonia 2021-2023.

1.4 Manfaat

1.4.1 Manfaat Teoretis

Penelitian ini diharapkan menjadi kontribusi dalam bahan pembelajaran serta penambah ilmu pengetahuan Hubungan Internasional (HI), khususnya pada pemahaman terhadap ancaman *cyber* sebagai bagian dari kajian keamanan.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan pandangan yang informatif kepada pembuat kebijakan (*policy maker)* dalam pembentukan atau perancangan kebijakan dalam menghadapi ancaman *cyber*.

II. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Dalam penelitian, peneliti merujuk pada 5 (lima) *literature review* sebagai bahan bacaan, referensi, dan informasi dalam penulisan yang berkaitan dengan tema. **Pertama,** jurnal yang berjudul *"Analysis of the 2007 Cyber Attack Against Estonia from the Information Warfare Perspective"* oleh Rain Ottis merupakan *Professor of Cyber Operations at TalTech* di Universitas Teknologi Talin, Estonia. Jurnal ini menjelaskan analisis terhadap kronologi serangan *cyber warfare* 2007 yang dialami Estonia. Rain Ottis menarik tiga hipotesis, yaitu: pertama serangan *cyber war* merupakan operasi propaganda informasi Rusia untuk melawan Estonia. Hal ini dikarenakan para tim penyelidik Rusia tidak bekerjasama dengan cukup baik dan terbuka. Yang kedua, serangan *cyber* yang berasal dari Rusia merupakan operasi bendera palsu untuk menjebak Rusia sebagai dalang dari serangan *cyberwar*. Ketiga, peristiwa *cyberwar* ini merupakan respon dari masyarakat Rusia dari kebijakan Estonia perihal pemindahan *The Bronze Soldier*. Lebih jauh lagi Rain Ottis menyebutkan bahwa, hanya dengan serangan *cyber* bisa membuat kehancuran suatu negara beserta infrastruktur atau aset negara yang berhubungan dengan internet tanpa menggunakan serangan militer.

Kedua, jurnal yang berjudul "*Cyber Deterrence: A Case Study on Estonia's Policies and Practice"* oleh Piret Perink merupakan pimpinan dalam organisasi keamanan *cyber* Estonia. dalam tulisannya menyoroti strategi yang diterapkan oleh Estonia untuk pencegahan pada serangan *cyber*. Studi ini pula menjelaskan

pentingnya untuk berkerjasama dengan sektor swasta. Penjelasannya adalah, bahwasannya swasta sangat penting untuk isu yang melibatkan transnasional. Poin pentingnya yang ingin ditunjukan adalah *cyber* Estonia sebagai coordinator untuk mengelola insiden *cyber* dan melakukan Latihan keamanan *cyber* secara berkala. Secara keseluruhan jurnal ini memberikan kontribusi untuk menawarkan tentang negara dalam mengembangkan kebijakannya pada penerapan strategi pencegahan *cyber* yang efektif.

Ketiga, Jurnal yang berjudul *"Russian Propaganda, Disinformation, and Estonia's Experience"* oleh Viljar Veebel merupakan *Chair of Humanities and Social Science,* di Sekolah Tinggi Pertanahan Nasional Estonia. Jurnal ini menjelaskan bahwa, sejak tahun 2000 Rusia sudah menerbitkan doktrin keamanan informasi, bertujuan untuk melindungi diri dari informasi asing yang mengancam Rusia. Doktrin tersebut ditujukan juga untuk membentuk rasa patriotisme rakyat Rusia. Namun propaganda dari doktrin keamanan informasi Rusia juga diarahkan kepada negara-negara lain. Hal tersebut dilihat dari sikap Rusia yang menolak untuk bergabung konvensi kejahatan terhadap dunia maya pada tahun 2001 yang diselenggarakan oleh Uni Eropa. Kemudian, berlanjut pada tahun 2007 munculnya peristiwa serangan *cyber* yang berasal dari Rusia merupakan, reaksi terhadap kebijakan pemindahan tugu *the bronze soldier* oleh pemerintah Estonia. Viljar Veebel menjelaskan agar menanggapi propaganda Rusia dengan cara Uni Eropa harus berinisiatif dalam mencurahkan sumber daya yang dimilikinya dalam artian lain adalah mencurahkan dana untuk menciptakan informasi dimaksudkan untuk terhindarnya dari respon prasangka yang diciptakan oleh propaganda.

Keempat, jurnal yang berjudul *"Russia Approach to Cyber Warfare"* oleh Michael Connel merupakan *Commercial Real Estate Lawyers,* dalam jurnalnya menjelaskan perkembangan taktik *cyber* pada negara Rusia sangat maju demikian bisa dilihat dari serangan kepada *server* Estonia, pembajakan DNS ke Georgia, dan terakhir meretas pembangkit listrik di Ukraina yang dilakukan oleh sindikat Ouroboros, yakni kelompok peretas. Akibatnya menyebabkan wilayah Krimea diambil alih oleh Rusia pada tahun 2014. Meskipun Rusia tidak terbukti secara kuat sebagai dalang serangan, tetapi sudah dipastikan Kremlin memberi fasilitas untuk adanya peluang serangan *cyber* melalui doktrin propaganda informasi

Rusia. Kremlin membagi dua kategori dalam menjalankan rencana doktrin tersebut, yakni:

1. Melakukan spionase melalui dunia maya dengan maksud mendapatkan informasi penting untuk melemahkan kekuatan politik negara musuh atau negara saing.
2. Melakukan *troll internet,* yakni sebuah usaha melakukan propaganda seperti menyerang akun media massa pemerintah negara musuh dan membentuk skenario pro Rusia.

Menurut James Clapper, tujuan dari tindakan perilaku tersebut semata-mata untuk menunjukkan kepada AS (Amerika Serikat) bahwa Rusia mampu melakukan serangan taktik *cyber* dan mampu bersaing di dunia maya.

Kelima, jurnal yang berjudul *"Cyberspace and the Changing nature of Warfare"* oleh Kenneth Geers, merupakan *U.S Representative* dari organisasi *Cooperative Cyber Defence Centre of Excellence*, Talin, Estonia. Dalam jurnalnya menjelaskan perkembangan sejarah *cyber* yang bermula dari jaringan TV kemudian terus berkembang sampai pada penggunaan internet. Tetapi hal yang harus dipahami dunia maya sudah masuk terhadap pada ranah konflik politik dan militer bahkan taktik penyerangan dunia maya dinilai lebih efektif dan tidak memerlukan biaya besar dibandingkan dengan taktik militer yang menggunakan persenjataan. Pada contoh kasus Estonia menjadikannya bukti dunia maya sudah termasuk sebagai ancaman terhadap keamanan nasional.

Tabel 2. 1 Perbandingan penelitian terdahulu

Peneliti Terdahulu	Judul	Teori dan Konsep	Metode Penelitian	Kesmipulan
Rain Ottis	*Analysis of the 2007 Cyber Attack Against Estonia from the Information Warfare Perspective*	Politik Internasional	Pendekatan Kualitatif	Dari tiga hipotesis yang dibentuk, ada satu kemungkinan yang dianggap paling masuk akal, yakni penjelasan terhadap operasi propaganda informasi Rusia, yaitu pemerintah memotivasi rakyatnya untuk melakukan serangan dengan cara apapun termasuk serangan *cyberwar* dan juga pemerintah bisa melindungi rakyatnya, sehingga ini menjelaskan alasan penyidik Rusia tidak bisa bekerjasama dengan baik kepada pemerintah Estonia.
Piret Perink	*Cyber Deterrence: A Case Study on Estonia's Policies and Practice"*	*Foreign Policy*	Pendekatan Kualitatif	Menyoroti strategi yang diterapkan oleh Estonia untuk pencegahan pada serangan *cyber*. sangat penting untuk isu yang melibatkan transnasional. Poin pentingnya yang ingin ditunjukan adalah *cyber*Estonia sebagai coordinator untuk mengelola insiden *cyber* dan melakukan Latihan keamanan *cyber* secara berkala. Secara keseluruhan jurnal ini memberikan kontribusi untuk menawarkan tentang negara dalam mengembangkan kebijakannya pada penerapan strategi pencegahan *cyber* yang efektif.
Viljar Veebel	*Russian Propaganda, Disinformation and Estonia's Experience*	Rezim Internasional dalam perspektif Institusionalisme	Pendekatan Kualitatif	Negara-negara Eropa harus mencurahkan sumber dayanya untuk membentuk sumber informasi yang didasari fakta sebagai pengelakan dari propaganda Rusia. Inisiatif Uni Eropa untuk melawan propaganda media Rusia merupakan langkah yang paling tepat, serta melakukan promosi kebebasan media pada negara mitra yang berada di Eropa Timur.
Michael Connel	*Russia Approach to Cyber Warfare*	*Strategic Power*	Pendekatan Kualitatif	Taktik *cyber* pada negara Rusia sangat maju demikian bisa dilihat dari serangan kepada *server* Estonia, pembajakan DNS ke Georgia, dan terakhir meretas pembangkit listrik di Ukraina yang dilakukan oleh sindikat Ouroboros yakni kelompok peretas. Akibatnya menyebabkan wilayah Krimea diambil alih oleh Rusia pada tahun 2014. Meskipun Rusia tidak terbukti secara kuat sebagai dalang serangan namun sudah dipastikan Kremlin memberi fasilitas untuk adanya peluang serangan *cyber* melalui doktrin propaganda informasi Rusia. Menurut James Clapper, tujuan dari tindakan perilaku tersebut semata-mata untuk menunjukkan kepada AS (Amerika Serikat) bahwa Rusia mampu melakukan serangan taktik *cyber* dan mampu bersaing di dunia maya.

Kenneth Geers	*Cyberspace and the Changing nature of Warfare*	*Non-traditional security*	Pendekatan Kualitatif	Konflik politik dan militer saat ini sudah memasuki dimensi dunia maya. Internet merubah semua hal tersebut. Kemajuan teknologi bisa menguntungkan negara-negara kuat begitu juga sebaliknya, internet bisa dimanfaatkan oleh pihak yang lemah sebagai senjata utama untuk menyerang negara-negara kuat dalam konvensionalnya. Seperti serangan teroris, siber dan taktik yang melibatkan non-konvensional lainnya, ini menjadi tugas tambahan untuk para pembuat kebijakan kemanan nasional.
Perbandingan Peneltian Penulis Dengan Penelitian Terdahulu	Aktor dalam sekuritisasi terhadap ancaman *cyber* di Estonia (2007-2023)	*Securitization, Cyber Threats/cyber*	Pendekatan Kualitatif	Mengkaji serangan *cyber* Estonia yang terjadi pada tahun 2007 dan juga pada masa kini, penulis soroti untuk masa kini pada rentan waktu 2021-2023 hal ini dimaksud untuk mengemukakan kasus ancaman dan focus sekuritisasi dengan mengemukakan actor-aktor sekuritisasi. Dengan tujuan dapat menganalisis keberlanjutan Estonia dalam menghadapi ancaman *cyber* terkait kasus serangan *cyber* 2007 dan 2023 dalam proses keamanan.

(Tabel diolah oleh peneliti)

2.2 Landasan Teori dan Konsep

Landasan teori atau konseptual yang digunakan dalam penelitian ialah menggunakan konsep *securitization* dan *cyber threats*, agar dapat membantu peneliti dalam menganalisis sekuritisasi terhadap ancaman *cyber* di Estonia terkait serangan *cyber* dari Rusia.

2.2.1 *Securitization*

konsep *securitization* mencakup pada permasalahan yang tidak berhubungan dengan aktor negara/*aktor state*, tetapi memiliki hubungan pada keamanan sosial dan berkaitan kuat dengan permasalahan kebebasan serta hak-hak sipil. Pada konteks ini, peran aktor *state* sangat penting dalam pengambilan tindakan keputusan. Secara sederhana mendefinisikan *securitization* sebagai kerangka untuk aktor negara bisa melewati batas-batas normal prosedur politik negara sebagai aktor yang dianggap perlu, tetapi pemahaman tersebut masih tidak bisa dimaknai sebagai definisi yang berfilosofi. *Securitization* atau sekuritisasi adalah proses pengamanan dari sebelumnya dianggap sesuatu yang tidak perlu diperhatikan karena, kondisi yang berubah sikap politisasi dari elit politik untuk mengambil keputusan sebagai bentuk keamanan yang harus dijaga. Membahas seputar sekuritisasi juga tidak jauh pula dengan terkait politisasi, karena *securitization* hanya pada dasar sebuah wacana permainan politik. Wacana politik yang digunakan sebagai alat untuk mengukur aktor negara dalam menjelaskan perilakunya yang menentukan suatu ancaman yang perlu dilakukan sekuritisasi atau tidak. Barry Buzan mendefinisikan konsep *Securitization* adalah kesadaran ancaman yang bersifat intersubjektif serta dipengaruhi efek politik substansial dan tidak memerlukan indikator Atau pengertiannya yang lebih tepat adalah *securitization* bukan memahami keamanan sebagai objektivitas karena sebuah proses pemahaman aktor dari rangkaian peristiwa untuk dipertimbangkan sebagai bentuk ancaman atau tidak (Barry Buzan, 1998). Terdapat tiga hal dalam analisis keamanan yang dikembangkan oleh Barry Buzan dan Weaver, yakni:

1. ***Referent object***: entitas dapat diidentifikasi sebagai objek yang terancam dan sebagai pusat dalam proses sekuritisasi. Ketika suatu isu dari *treat object* tersebut diangkat sebagai ancaman. Sehingga entitas tersebut merasa perlu untuk mengambil arah tindakan dalam melakukan pertahanan dan perlindungan dari ancaman. Hal ini sebagai maksud

untuk mempertahankan eksistensinya dengan memahami posisi entitas yang bertujuan agar mendapatkan perhatian *audience* terhadap suatu objek ancaman.

Buzzan memberikan identifkasi untuk mengkategorikan analisis *referent object,* yakni:

- Negara

  Dalam penjelasannya Negara sering kali menjadi *referent object*, karena dalam kajian keamanan tradisional ancaman berupa integritas teritotial, kedaulatan dan kemampuan Negara dalam menjalankan keamanan. Keamanan Negara merupakan *referent object* utama untuk dipertahankan entitasnya. Ancaman terhadap Negara merupakan eksistensial yang dapat munculnya disintegritas atau kehilangan wilayah. Peran *referent object* dalam politik keamanan Negara adalah menjaga stabilitas politik Negara untuk keberlangsungan entitas politik.

  Seperti, kudeta militer, pemberontakan senjata yang bertujuan untuk meruntuhkan pemerintahan. Ancaman ideologis juga dapat dianggap sebagai ancaman terhadap *referent object* Negara. Misalnya, melakukan propaganda asing atau melakukan afiliasi ideology yang bertentangan. Pada konteksnya keamanan tidak hanya berfokus pada ancaman militer, melainkan ancaman yang lebih komprehensif terhadap ancaman.

- *Society* (Masyarakat Sosial)

  Society atau masyarakat sosial mengarah kepada masyarakat sebagai *referent object* dalam hal ini mengacu identitas kolektif nilai budaya atau cara hidup suatu kelompok. Ancamannya merujuk pada upaya untuk mengubah, menghancurkan identitas dan nilai-nilai yang dianggap penting yang dianggap dapat menghilangkan kultural ciri khas bagi kelompok tersebut. Nilai-nilai tersebut bisa mencakup bahasa, budaya, adat, dan agama yang membentuk karakteristik suatu kelompok masyarakat. Ancaman ini bisa berasal dari perbedaan

tersebut atau tekanan eksternal lainnya yang menggangu keseimbangan sosial-politik dengan merusak identitas masyarakat kelompok sosial.

Contoh ancaman pada *referent object* masyarakat social, seperti migrasi. Ini adalah salah satu ancaman yang dihadapi keamanan masyarakat social, karenadapat mengubah komposisi demografis dan dapat merusak identitas kolektif komunitas. Kemudian ada juga isu globalisasi, isu ini membawa ancaman terhadap nilai-nilai adat istiadat local melalui penyebaran budaya yang dominan. Hal ini mengancam pada pengikisan budaya pada masyarakat social, sehingga menyebabkan krisis identitas pada suatu komunitas.

- *Individual*

Referent object ini penting dilindungi dari ancaman yang berupa perlindungan terhadap kehidupan, kebebasan, dan HAM (Hak Asasi Manusia. Penekanan keamanan individu sebagai *referent object*, yakni mencakup keamanan dalam memberikan perlindungan individu tersebut pada kekerasan, pelanggaran HAM, dan kelayakan individu dalam kondisi hidup. Ancaman ini bisa hadir dari berbagai arah, seperti dari hasil tindakan aktif Negara, yakni konflik bersenjata dan kebijakan Negara yang merugikan individu manusia, selain Negara bisa juga hadir dari kelompok kekerasan non-negara.

- Ekonomi

Referent object pada ekonomi, yakni tercakup pada sistem ekonomi pada industri, infrastruktur, dan perusahaan ekonomi vital yang dapat memberi kelangsungan hidup Negara dan masyarakatnya. Ekonomi yang stabil dapat member pilar pada kesejahteraan Negara dalam member kehidupan masyarakatnya. Keamanan ekonomi terhadap ancamannya bisa berasal baik dari internal maupun eksternal. Ancaman bisa dalam bentuk krisis financial yang menyebabkan penurunan ekonomi, sehingga mengarah pada pengganguran missal dan menyeybabkan menurunnya daya beli. Ada juga dari eksternal, seperti

embargo ekonomi, yaitu pembatasan ekonomi ke suatu Negara dari Negara lainnya. Tindakan ini membuat kondisi suatu Negara dapat menggalami tekanan yang bisa menyebabkan aktifitas perputaran ekonomi Negara tidak bergerak dan merugikan rakyatnya.

- Lingkungan

Pada bagian ini memperkenalkan *referent object* dari keamanan lingkungan. Ini menyoroti pentingnya lingkungan sebagai komponen kunci dalam keamanan sekuritisasi. Lingkungan sebagai *referent object* didefinisikan sebagai perlindungan ekosistem dan sumber daya alam dari ancaman yang dapat menyebabkan kerusakan. Dalam konteks keamanan, focus utamanya adalah mengupayakan keberlanjutan lingkungan yang meliputi, ekosistem alam, sumber daya alam, keaekaragaman hayati, dan kesehatan lingkungan. Keberadaan lingkungan dianggap penting karena, inilah yang memberikan keberlangsungan hidup semua elemen, baik Negara, manusia, bahkan *society* membutuhkan keberlangsungan lingkungan.

Dengan demikian, peran penting *referent object* pada sekuritisasi, khususnya pada isu *cyber attack* di Estonia pada tahun 2021-2023 sebagai rujukan dalam melindungi entitas yang dianggap penting dan harus dilindungi dari ancaman. Dalam kasus Estonia, hal-hal yang harus diperhatikan adalah, mencakup berbagai dimensi, seperti keamanan nasional, social hingga kedaulatan digital. Ancaman ini pula dapat membahayakan stabilitas politik Estonia. melalui pemahaman mendalam tentang *referent object*, actor-aktor yang terlibat dalam sekuritisasi dapat dirumuskan dan bisa mengimplementasikan keamanan terhadap perlindungan dalam keberlanjutan Negara di era digital.

2. ***Securitizing aktors:*** aktor yang melakukan upaya sekuritisasi untuk mendefinisikan suatu isu sebagai ancaman dengan melakukan klaim atau deklarasi terkait *threat object* untuk mengesahkan isu sebagai ancaman. Aktor dalam alat analisis ini mengarahkan untuk meyakinkan dan

kerjasama dengan *audience* dalam usaha sekuritisasi terhadap sebuah isu objek ancaman. Selain itu, *securitizing aktor* adalah seorang *aktor* individu. Dalam hal ini *securitizing aktor* dalam membujuk *audience* melakukan pemanfaatan *speech act,* yang dimana ini adalah tindakan komunikatif yang bertujuan untuk merubah persepsi tentang keamanan dan mendorong tindakan aktor untuk menciptakan narasi tentang ancaman. Hal ini akan mempengaruhi *audience* dalam merespon isu yang sama sebagai ancaman, selain itu utuk mendapatkan perhatian *audience, securitizing actor* memiliki karakteristik agar melancarkan *speech act.*

a) *Audience*

Audience adalah pihak yang ditargetkan actor *securitizing actor* untuk meyakinkan isu yang diangkat merupakan ancman serius. Keberhasilan *securitizing actor* sangat tergantung dengan dungkan *audience*. Tanpanya upaya sekuritisasi tidak berhasil. Peran dari *audience* meliput adanya legitimasi, maksudnya dengan *audience* memberikan legitimasi kepada *securitizing actor*.

b) *Speech Act*

Speech act adalah tindakan komunikatif yang digunakan oleh *securitizing actor* sebagai pernyataan pada isu ancaman. *Speech act* memuat pernyataan melalui deklarasi atau pidato untuk meyakinkan *audience.*

c) *Karakteristik*

karakteristik yang dimiliki *securitizing actor*, yakni

- Otoritas dan legitimasi, karakteristik ini agar bisa diakui oleh *audience.*
- Kredibilitas, karakteristik ini agar dipercaya oleh *audience* dalam klaim pada suatu isu ancaman.
- Akses Komunikasi, karakteristik ini agar dapat menyebarkan pesan isu ancaman secara efekti kepada *audience*.

3. ***Functional aktors***: aktor individu yang pada bagiannya adalah secara tidak langsung terlibat dalam mengatasi ancaman dan penting dalam *decision* terhadap ancmaan. Menentukan atau mengidentifikasi *functional aktor,* yaitu individu atau entitas yang memiliki kekuatan dalam mempengaruhi militer, Dalam hal ini mereka yang terpenting adalah memiliki pengaruh militer, yang mengarah kepada kebijakan militer. Meskipun perannya tidak seperti *audience* di *securitizing actor,* fungsi pada actor ini adalah bersifat fungional dan teknis.

   Functional actor memiliki karakteristik sebagai berikut:

   - Pengaruh, adalah karakteristik untuk memberikan pengaruh secara tidak langsung dalam mendefinisikan isu ancaman dan mempengaruhi tindakan mengatasi masalah ancaman. Contohnya, seperti pengembangan solusi dalam menghadapi ancaman.
   - Teknis dan operasional, yakni memberikan kontribusi dalam hal teknis dan operasional dalam penangan ancaman. Sebagai contoh, penyediaan alat-alat atau layanan untuk menyikapi isu pada ancaman.
   - Peran dalam kapabilitas infrastruktur, yakni berperan pada infrastuktur yang diperukan untuk menghadapi ancaman. Sebagai contoh, pembentukan lembaga riset teknologi pertahanan dan penambahan institusi pendidikan tenaga ahli untuk menghadapi isu ancaman.

Dengan demikian keterkaitan antara konsep *securitization* dengan penelitian adalah, untuk mengidentifikasi dan menganalisis actor dalam sekuritisasi di Estonia. studi ini pula menyoroti pentingnya kolaborasi antara actor keamanan dalam membentuk persepsi dan respons terhadap ancaman *cyber*. Secara keseluruhan, konsep ini memberikan alat analisis untuk mengidentifikasi actor terkait yang berperan dalam isu *cyber*.

2.2.2 Cyber Attack

Dalam upaya memahami fenomena *cyber attack* ada 2 literature dari beberapa tokoh yang peneliti ambil guna membantu menjabarkan definisi *Cyber Attack* untuk menjelaskan pengertian yang relevan untuk membantu menjelaskan isu *cyber attack* sebagai berikut:

- Singer dan Friedman

  Didalam bukunya yang berjudul "*cybersecurity and cyberwar: what needs to know"* mendefinisikan *cyber attack* sebagai tindakan penipuan yang disenggaja untuk merusak dan menghancurkan system computer atau jaringan, serta informasi yang termuat didalamnya.

- Clarke dan Knake

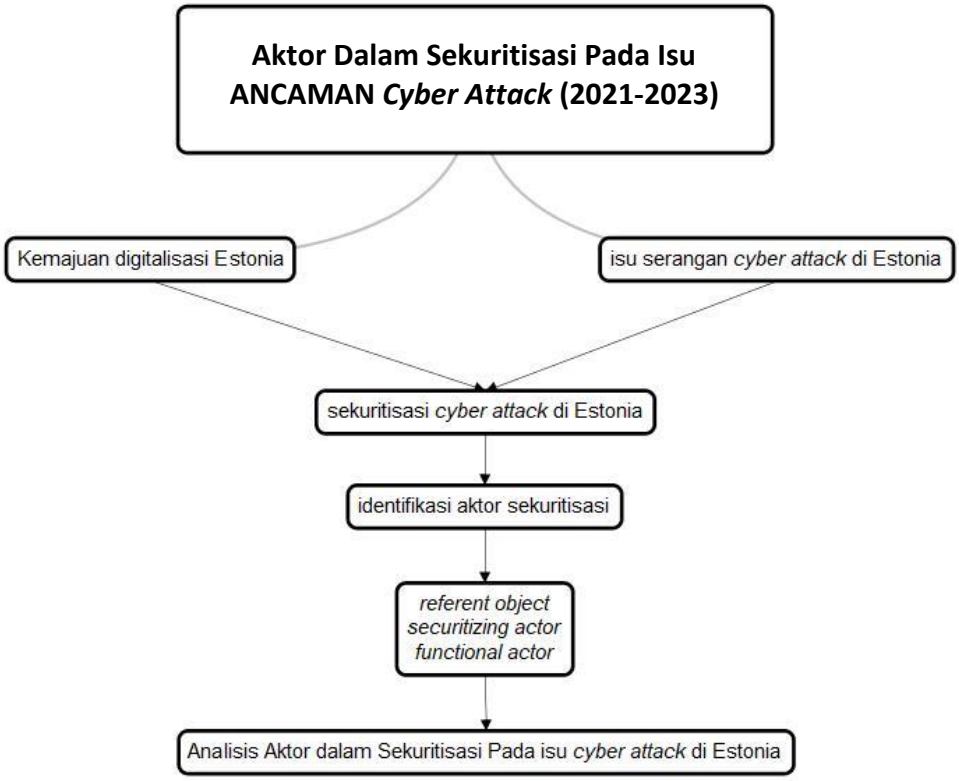
  Didalam tulisannya yang berjudul *"the fifth domain: defending our country, our companies, and ourselves in the age of cyber threats"* menggambarkan *cyber attack* sebagai maneuver untuk menargetkan system informasi computer, infrastruktur, jaringan atau perangkat computer pribadi untuk tindak peretasan system yang bertujuan pencurian, mengubah atau menghancurkan.

Pada definisi yang dijabarkan dari dua literature, semua sumber sepakat, bahwa *cyber attack* adalah tindakan yang merugikan dengan menargetkan system computer dan jaringan, sedangkan perbedaan dari keduanya ialah pada buku yang ditulis Singer dan Friedman menekankan aspek penipuan dan kerusakan. Pada tulisan karya Clarke dan Knake menjabarkan pada system yang rentan untuk diretas. Penelitian ini menggunakan definisi tersebut untuk membangun kerangka analitis dalam mengkaji *cyber attack* sebagai ancaman oleh sekuritisasi di Estonia pada periode 2021-2023

2.3 Kerangka Pemikiran

Untuk menjawab pertanyaan penelitian mengenai aktor-aktor yang terlibat dalam sekuritisasi terhadap isu *cyber attack* di Estonia 2021-2023, penelitian menggunakan kerangka pemikiran yang melibatkan konsep *securitization* dan *cyber*

attack. Secara historis, konsep *securitization* digunakan untuk menganalisis Aktor yang terlibat dalam proses keamanan dalam menghadapi ancaman. Disisi lain, konsep *cyber attack* digunakan untuk menjelaskan fenomena yang terjadi pada periode 2021-2023. Dengan menganalisis aktor yang terlibat dalam sekuritisasi terhadap ancaman *cyber* di Estonia, penelitian ini dapat memberikan pemahaman untuk upaya Estonia dalam menghadapi ancaman isu *cyber attack* dalam konteks *securitization.*



(gambar diolah oleh peneliti)

Gambar 2. 1 Kerangka Pemikiran

III. METODE PENELITIAN

3.1 Jenis Penelitian

Pada penelitian ini penulis menggunakan pendekatan jenis penelitian kualitatif deskriptif. Pendekatan kualitatif merupakan jenis penelitian yang memahami dan mengenali subjek pada tindakan perilaku sosial masyarakat. Pendekatan kualitatif juga merupakan jenis penelitian yang meneliti kehidupan masyarakat, sejarah, tingkah laku, serta gerakan sosial. Penelitian kualitatif umumnya merupakan penelitian yang menggunakan studi kasus. Menurut Yin, penelitian studi kasus merupakan upaya generalisasi temuan yang didapat dari suatu kasus (Creswell, 2009). Oleh karena itu penelitian ini mendeskripsikan, memahami, serta menganalisis hal-hal yang berkaitan dengan aktor-aktor yang terlibat dalam sekuritisasi terhadap isu *cyber attack* di Estonia.

3.2 Fokus Penelitian

Penelitian ini berfokus pada eksplanasi dari aktor sekuritisasi untuk menyikapi gejolak peristiwa serangan *cyber*. Hal tersebut dijelaskan melalui adanya perilaku aktor dalam melakukan sekuritisasi terhadap ancaman *cyber attack,* sebagai respon pada peristiwa serangan *cyber* kepada Estonia.

3.3 Jenis dan Sumber Data

Pada penelitian ini jenis data yang digunakan adalah jenis data sekunder atau data yang didapat merupakan hasil dari penelitian sebelumnya atau dari pihak kedua. Sumber data penelitian diperoleh dari studi literasi beberapa situs berita

resmi tentang penyebab serangan *cyber* ke Estonia, dokumen-dokumen jurnal riset terdahulu oleh lembaga kajian atau *think tank* dan juga dari organisasi CCDCoE berisikan analisis dari peristiwa serangan *cyber warfare* tersebut yang tersedia pada laman website resmi Foreign Policy Research Institute pada *link www.fpri.org*, Center for Strategic & International Studies dengan *link www.csis.org*, Cooperative Cyber Defence Centre of Excellence dengan *link www.ccdcoe.org*, serta dokumen laporan pemerintah Estonia melalui laman E-Estonia dengan *link e-estonia.com*, untuk memperkaya data pada penelitian. Data-data tersebut digunakan dalam penelitian.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data merupakan proses atau tatanan pengumpulan data yang dilakukan oleh peneliti untuk membatasi ruang lingkup riset agar berfokus pada pertanyaan penelitian. Dengan menggunakan pendekatan kualitatif, teknik pengumpulan yang diambil ialah dengan mengkaji literasi bacaan *(content analysis)* dari buku, jurnal riset, surat kabar atau media berita yang berkaitan dengan pembahasan *Securitization* pada buku dari karya Barry Buzan, dan jug yang berkesinambungan dengan kasus serangan *cyber* di Estonia, melalui laman website E-estonia, CCDCoE, FSPI, CSIS.

3.5 Teknik Analisis Data

Proses teknik analisis data melibatkan pengurutan dalam pemilahan data dan diolah dan disusun untuk mendukung hipotesis penelitian. Penelitian ini mengadopsi metode teknik analisis data yang diusulkan oleh Miles dan Huberman. Menurut Miles dan Huberman tahun 2014 metode teknik analisis data terdiri dari:

1. Kondensasi Data

   Peneliti melakukan analisis dengan penyederhanaan data temuan dan memadatkannya untuk mencegah adanya data yang terbuang selama proses penelitian untuk memfokuskan temuan penelitian. Tujuannya

supaya dapat menyajikan data dari berbagai sumber dengan lebih tajam dan fokus pada penelitian.

2. Penyajian Data

Pada tahap ini, peneliti menyusun data dan informasi yang diperoleh untuk disesuaikan berdasarkan teori atau konsep yang digunakan dalam penelitian dalam bentuk deskriptif, grafik, dan tabel. Hal ini bertujuan agar membantu memahami dan memfasilitasi penarikan kesimpulan pada penelitian.

3. Penarikan Kesimpulan.

Ditahapan ini, setelah data diolah dan dianalisis, kemudian disajikan secara efektif sesuai dengan topik penelitian berlandaskan teori dan konsep, selanjutnya dilakukan penarikan kesimpulan sebagai maksud untuk menjawab pertanyaan penelitian atau rumusan masalah.

V. SIMPULAN DAN SARAN

5.1 Simpulan

Analisis aktor sekuritisasi melibatkan *referent object, securitizing aktor,* dan *functional aktor*. Analisis penelitian tentang aktor-aktor yang terlibat dalam sekuritisasi di Estonia pada tahun 2020-2023, terdapat temuan berupa, serangan *cyber* 2021-2023. Serangan yang terjadi berupa DDoS, *Phishing,* dan *ransomware.* Ini menunjukan serangan *cyber* terus berkembang dan merupakan ancaman serius bagi Estonia. Analisis sekuritisasi ancaman *cyber* pada masa kini (2023) melibatkan *referent object* Estonia sebagai eksistensi Negara yang berdaulat dan anggota NATO, *securitizing aktor* Alar Karis dan Kalla Laanet dengan *speech act* yang dilakukan membuat perhatian *audience* untuk menganggap *cyber* sebagai ancaman, yaitu pemerintah Estonia dan organisasi NATO, dan terakhir adalah *functional aktor*, melalui CERT yang berperan untuk meningkatkan kewsapadaan pada ancaman *cyber* tetap tinggi. Dari hasil penelitian ini, menjelaskan ancaman *cyber* meruakan ancaman nyata bagi Estonia, upaya-upaya sekuritisasi yang dilakukan merupakan buah dari yang diusahakan oleh aktor-aktor sekuritisasi. Ini mengartikan keseriusan para aktor untuk mau terlibat dalam melawan ancaman ini. Diperlukan kerjasama internasional dalam mengatasi isu ancaman *cyber*, seperti dengan NATO, Negara lain, dan juga pihak swasta untuk meningkatkan keamanan *cyber.*

5.2 Saran

Ancaman *cyber* ini bisa menimpa negara manapun bahkan, Estonia yang sudah lebih unggul dan maju dalam digitalisasi masih saja bisa terkena serangannya. Terlepas pemicunya adalah tentang isu etnis yang mengartikan *cyber* bisa menjadi alat politik dan untuk kemungkinan terburuknya adalah bisa dijadikan alat perang. Hal tersebut dimaksudkan pada negara yang belum fokus pada keamanan *cyber* untuk juga melihat *cyber* sebagai ancaman serius. Peneliti menyarankan kepada *policy maker* pada negara yang masih belum berfokus pada *cyber* untuk melakukan investasi lebih kepada *cyber defence* dibandingkan hanya berfokus pada peningkatan militer saja. Bukan berarti peneliti meremehkan keamanan militer, melainkan seperti yang dikatakan oleh Gerasimov, yakni peran dari nonmiliter terhadap militer sebesar 4:1. Ini menjelaskan betapa besarnya ancaman dari nonmiliter seperti *cyber*.

Peneliti menyadari pada kelemahan penelitian, yakni peneliti acap kali menemukan data yang berpihak maksudnya, data-data yang ditemukan sering kali menyudutkan Rusia sebagai pelaku utama dalam serangan *cyber* yang tidak terbukti bahkan, data dari organisasi terpercaya sekalipun. Penelitian ini dikerjakan dengan pemikiran yang netral atau tidak berhihak dengan maksud untuk perhatian kita berfokus pada seriusnya ancaman *cyber* ini. Oleh karena itu diharapkan jika ada peneliti selanjutnya yang akan melanjutkan penelitian tentang keamanan *cyber*, agar menemukan dan menerima data dengan beberapa sudut pandang, agar menghindari keberpihakan dalam mengemukakan argumentasi.

DAFTAR PUSTAKA

Aaviksoo, J. (2020, June 0). *Academia Scientiarum Estoniae*. Retrieved from Akadeemia Wesite: https://www.akadeemia.ee/en/member/aaviksoo-2/

Arbianita, R. L. (2024). *https://www.cert.or.id/tentang-kami/id/*. Retrieved from COMPUTER EMERGENCY RESPONSE TEAM: https://www.cert.or.id/tentang-kami/id/

Arnim Langer, G. K. (2012). Elgar Handbook of Civil War and Fragile States. In G. K. Arnim Langer, *Elgar Handbook of Civil War and Fragile States* (p. 16). Cheltenham, UK: Edward Elgar.

Authority, E. I. (2021). *Cyber Security in Estonia: Annual Report 2021*. Government of Estonia.

Barry Buzan, d. (1998). London: Lynne Rienner.

Barry Buzan, d. (1998). *Securitiy: A New Framework For Analysis.* London: Lynne RiennerPublisher, Inc.

CES. (2022). *Center for Europeanstudies.* Retrieved from UNC CES Web Site: https://europe.unc.edu/iron-curtain/history/the-fall-of-the-soviet-union/

Chalk, P. (2000). *Non-military Security and Global Order.* New York: ST Martin's Press.

Chertkov, A. (2021, September 9). *Estonian History and Culture*. Retrieved from Visit Estonia Website: https://www.visitestonia.com/en/why-estonia/estonian-history-and-culture

CNN Indonesia. (2023, May 09). *Internasional*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/internasional/20230509115337-106-947120/jokowi-sindir-china-soal-lcs-klaim-tak-berdasar-tak-boleh-terjadi

Creswell, J. W. (2009). *Research design: qualitative andmixed methods approaches (ed 3).* Los Angeles: SAGE Publication.Inc.

education estonia. (2022, March 30). *education estonia*. Retrieved from esucation estonia.org: www.educationestonia.org/cyber-security-education-in-estonia/

Eer News. (2023, June 1). *President Karis: Cyber security must involve whole of society*. Retrieved from https://news.err.ee/1608995129/president-karis-cyber-security-must-involve-whole-of-society

e-Estonia. (2022). *Building a digital society*. Retrieved from e-Estonia: https://e-estonia.com/solutions/

e-estonia. (2022). *estonia.ee*. Retrieved from estonia.ee web site: https://estonia.ee/oveview/

Emma, M. (2013, Maret 12). *Kementerian Pertahanan Republik Indonesia*. Retrieved from Kemhan Website: https://www.kemhan.go.id/badiklat/2013/03/12/sejarah-awal-berdiri-negara-rusia.html

Eneken. (2018). *From Cyber Defence to Cyber Security in Estonia.*

Estonian Information System Authority. (2024). *Estonian Information System Authority*. Retrieved from https://www.ria.ee/en/cyber-security/cert-ee.html

Europa Direct Strasbourg. (2021). *Centre d'Information sur les Institutions Européennes*. Retrieved from Europa Direct Strasbourg: https://www.strasbourg-europe.eu/estonia/#:~:text=1917%20Following%20the%20Russian%20Revolution,a%20democratic%20and%20liberal%20regime.

European Affairs. (2008). *The European Institute.* Retrieved from EuripeanIntitute.org: https://www.europeaninstitute.org/index.php/archive/sort-by-date-2/24-winterspring-2008/67-cyber-war-i-estonia-attracked-from-russia

Ewing, E. T. (2017, maret 13). *Perspectives on History*. Retrieved from Perspectives on History Web site: https://www.history.org/publications-and-directories/perspectives-on-history/march-2017/why-study-russian-history

Geers, K. (2008). Cyberspace and The Changing Nature of Warfare. *CCDCoE*, 8.

Gerasimov, V. (2013). *Nilai Ilmu Pengetahuan Ada di Masa Depan.*

Gerasimov, V. (2013). The Value of Science Is in the Foresight. *Military Review*, 28.

Gjelten, T. (2011, January 4). *npr*. Retrieved from npr.org: https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation

Gjelten, T. (2011, January 4). *Volunteer Cyber Army Emerges In Estonia*. Retrieved from NPR: https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation

Gori, U. (2009). *Modelling Cyber Security : Approach, Methodology, Strategies.* Venice: IOS Press BV.

Green, J. A. (2015). *Cyber Warfare A Multidisciplinary Analysis (Ed).* New York: Routledge.

Herzog, S. (2011). Revisiting the Estonia Cyber Attack : Digital Threats and Multinational Responses. 50.

Information System Authority. (2021). *Annual Cyber Security Report.*

Isabelle Drake, D. C. (Director). (2013). *Apocalypse Ep 5 - World War I - Dileverance* [Motion Picture].

Jaak Aaviksoo, d. (2010). Cyberattacks againts Estonia Raised Awarness of Cyberthreats. *Defence Againts Terrorisme Review: DATR*, 13-22.

Jigle, W. (2016, May 03). *DGAP*. Retrieved from DGAP.org: https://dgap.org/en/event/russkiy-mir-russian-world

Kaitseliit. (n.d.). *Kaitseliidu missioon, visioon ja väärtused*. Retrieved from Kaitseliit.ee: https://www.kaitseliit.ee/et/visioon-ja-vaartused

kaitseministeerium. (2021, April 15). Retrieved April 21, 2024, from Republik of Estonia Ministry of Defence: https://www.kaitseministeerium.ee/en/news/nato-cyber-pledge-2021-speech-kalle-laanet-minister-defence

Kamusella, T. (2018, February 9). *New Eastern Europe*. Retrieved from neweasterneurope.ue: https://neweasterneurope.eu/2018/02/09/russian-re-ethnicisation-pluricentrisme/

Kolesnikov, A. (2017). A Past That Divides: Russia's New Official History. *Carnegie Moskow Center*, 1.

KOMPASTV (Director). (2020). *Soal Natuna, Jokowi: Tidak Ada Tawar-Menawar!* [Motion Picture].

Kozlowski, A. (2014). *Europan Scientific*.

Kozlowski, A. (2014). COMPARATIVE ANALYSIS OF CYBERATTACK ON ESTONIA, GEORGIA AND KYRGYZSTAN. *Europan Scientific*, 2-4.

Lambert, T. (2021, Maret 14). *Local Histories*. Retrieved from Local Hitoris Web Site: https://localhistories.org/a-brief-history-of-estonia

Lieven, D. (2022, 4 2). *Britannica*. Retrieved from Britannica Web site: https://www.britannica.com/place/Russia

Lufkin, B. (2017, October 20). *BBC FUTURE*. Retrieved from BBC FUTURE Web site: https://www.bbc.com/future/article/20171019-could-estonia-be-the-first-digital-country

Miles, M. B. (2014). *Qualitative Data Analysis (Ed 3).* London: SAGE Publication.Inc.

Ministry of Defence. (2008). *Cyber Security Defence.* Talinn.

Ministry of Defence. (2008). *Cyber Security Strategy.* Tallinn.

Ministry of Defence of Estonia. (2019). Estonian National Security Concept. Ministry of Defence of Estonia.

Muhamad, S. V. (2020). ESKALASI KETEGANGAN DI LAUT CHINA SELATAN. *INFO Singkat Pusat Penelitian*, 8-10.

NATO. (1949). *The North Atlantic Treaty.*

NATO. (2022, June 3). *North Atlantic Treaty Organization*. Retrieved from NATO.int: https://www.nato.int/cps/en/natohq/declassified_139339.htm

NATO. (2023, Aug 3). *Topic: Relations with Russia*. Retrieved from NATO.int: https://www-nato-int/cps/en/natolive/topics_50090.htm?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

NATO.int. (2024, March 21). *Relations with the European Union*. Retrieved from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natolive/topics_49217.htm

OECDilibrary. (2019). *Chapter 13. Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation*. Retrieved from OECDilibrary: https://www.oecd-ilibrary.org/sites/510a82b5-en/index.html?itemId=/content/component/510a82b5-en

Office of the Historian, Foreign Service Institute. (2016). *Office of The Historian.* Retrieved from Office of The Historian Website: https://history.state.gov/milestones/1989-1992/collapse-soviet-union

Osula, A. M. (2015). *Nation Cyber Security Organization: Estonia.* Talilnn: ccdcoe.

Ottis, R. (2008). Analaysis of the 2007 Cyber Attack Againts Estonia from the Information Warfare Perspective. *Cooperative Cyer Defence Centre of Excellence* .

Ottis, R. (2011). Estonian Cyber Defence League: A Public-Private Partnership Model. International Journal of Cyber Warfare and Terrorism.

Permanent Structured Cooperation. (2021). Retrieved from https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

Piirmets, E. (2023, March 7). *e-government*. Retrieved from Enterprise Estonia: https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/

Prabook. (2020, nn 00). *Prabook*. Retrieved from Prabook website: https://prabook.com/web/mobile/#!profile/1762610

president.ee. (2021). *Alar Karis*. Retrieved from https://president.ee/en/republic-of-estonia/heads-of-state/31267-31267-alar-karis

PubAffairs Bruxelles. (2022). *PubAffairs Bruxelles.* Retrieved from PubAffairs Bruxelles.eu : https://www.pubaffairsbruxelles.eu/eu-institution-news/cyber-defence-meps-call-for-better-european-cooperation

Radio Free Europe Radio Liberty. (2007, May 9). *Estonia: Defense Minister Says Bronze Soldier Had To Go* . Retrieved from Radio Free Europe Radio Liberty: https://www.rferl.org/a/1076363.html

raud. (2021). *The Role of CERT in Cybersecurity: The Estonian Experience.*

Republic of Estonia. (2023). *Cyber Security in Estonia 2023.* Estonia.

Republic of Estonia. (2024). *Cyber Security in stonia.* Talinn: National Cyber Security.

Republic of Estonia Defence Forces. (2021, July 20). *Estonia Defence Forces*. Retrieved from Republic of Estonia Defence Force Web site: https://mil.ee/en/defence/forces/

Rid, T. (2013). *Cyber War Will Not Take Place.* New York: Oxford University Press, Inc.

Ringvaade, E. (2010). Estonian Review. *Foreign News*, 5.

SARI, D. L. (2019). STRATEGI ANCAMAN PERANGKAT HIBRIDA RUSIA: SEBUAH PERSEPSI DAN MANIFESTASI KEBIJAKAN ESTONIA. *Revie Hubungan Internasional*, 48.

Shalhoub, Z. K. (2010). *CybeLaw and Cyber Security in Developing and Emerging Economies.* Cheltenham: FSC Mixed.

Smith. (2010). Estonia's Defense Strategy: A Response to Internal Turmoil. *Journal on Baltic Security*, 45.

Stranga, A. (2022, 4 5). *Britannica*. Retrieved from Britannica.org: https://www.britannica.com/place/Estonia

UNHCR. (2023, 5 31). *Estonia: Treatment of ethnic minorities*. Retrieved from Refworld: https://webarchive.archive.unhcr.org/20230603142718/https://www.refworld.org/docid/3ae6ad4314.html

valitsus.ee. (2023). *Kalle Laanet*. Retrieved from Republic of Estonia Government: https://valitsus.ee/en/prime-minister-ministers/minister-justice-kalle-laanet

Veebel, V. (2015). RUSSIAN PROPAGANDA, DISINFORMATION, AND ESTONIA'S EXPERIENCE. *Foreign Policy Research Institute*, 2-3. Retrieved from https://www.fpri.org/article/2015/10/russian-propaganda-disinformation-and-estonians-experience

Vogler, M. C. (2017). Russia's Approach to Cyber Warfare. *CNA Analysis & Solution*, 3-4.

Waszczkowski, W. (2015). *The Battle for The Heart and Minds: Countering Propaganda Attack Againts The Euro-Atlantic Community.* NATO Parlementry.

Yee, A. (2022, 2 5). *BBC NEWS INDONESIA*. Retrieved from BBC FUTURE: https://www.bbc.com/indonesia/vert-fut-60227813