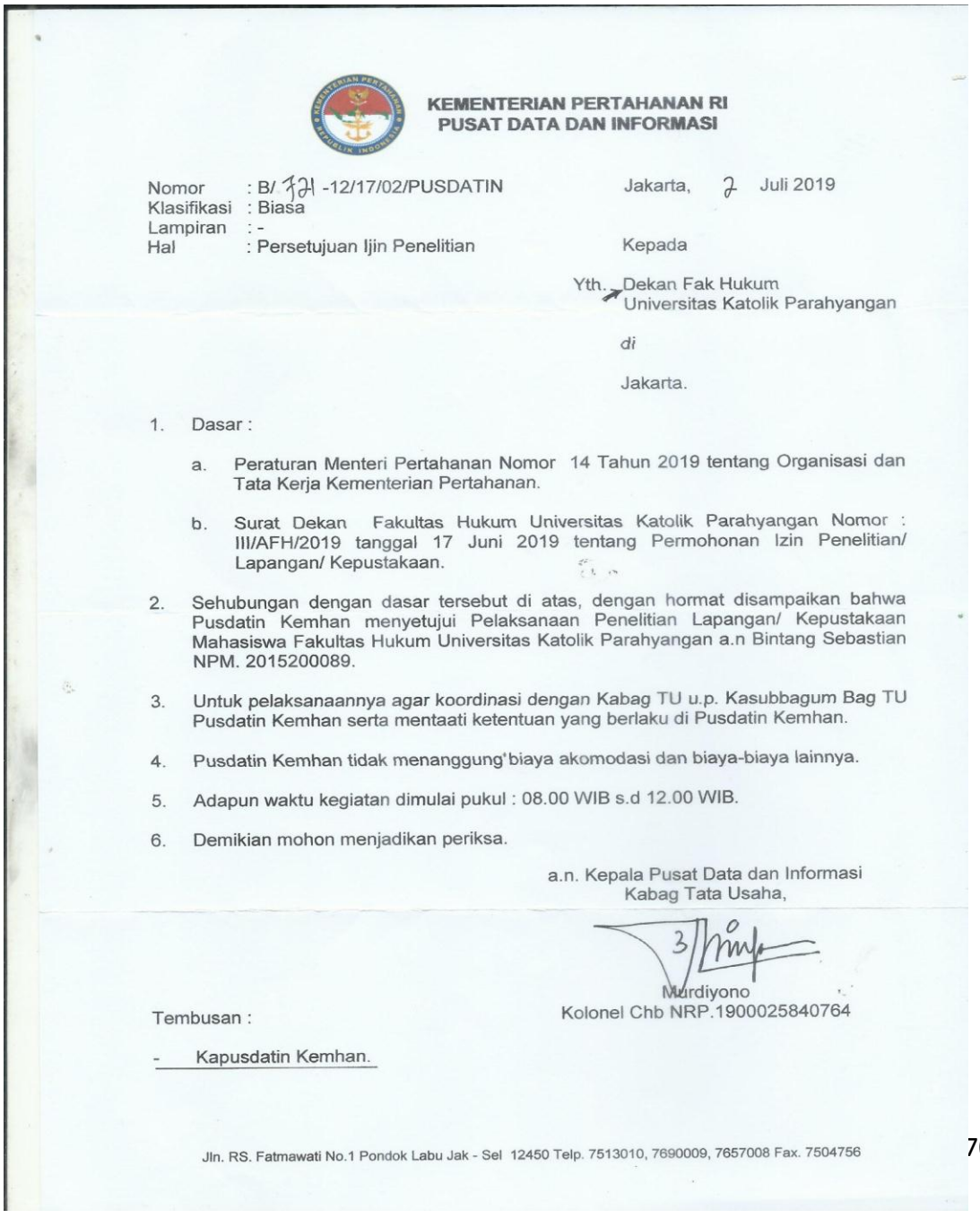
Lampiran I (Izin Penelitian di Pusat Data dan Informasi Kementerian Pertahanan)



KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

Nomor : B/ 721 -12/17/02/PUSDATIN
Klasifikasi : Biasa
Lampiran : -
Hal : Persetujuan Ijin Penelitian

Jakarta, 2 Juli 2019

Kepada

Yth. Dekan Fak Hukum
Universitas Katolik Parahyangan

di

Jakarta.

1. Dasar :
   a. Peraturan Menteri Pertahanan Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan.
   b. Surat Dekan Fakultas Hukum Universitas Katolik Parahyangan Nomor : III/AFH/2019 tanggal 17 Juni 2019 tentang Permohonan Izin Penelitian/ Lapangan/ Kepustakaan.
2. Sehubungan dengan dasar tersebut di atas, dengan hormat disampaikan bahwa Pusdatin Kemhan menyetujui Pelaksanaan Penelitian Lapangan/ Kepustakaan Mahasiswa Fakultas Hukum Universitas Katolik Parahyangan a.n Bintang Sebastian NPM. 2015200089.
3. Untuk pelaksanaannya agar koordinasi dengan Kabag TU u.p. Kasubbagum Bag TU Pusdatin Kemhan serta mentaati ketentuan yang berlaku di Pusdatin Kemhan.
4. Pusdatin Kemhan tidak menanggung biaya akomodasi dan biaya-biaya lainnya.
5. Adapun waktu kegiatan dimulai pukul : 08.00 WIB s.d 12.00 WIB.
6. Demikian mohon menjadikan periksa.

a.n. Kepala Pusat Data dan Informasi
Kabag Tata Usaha,

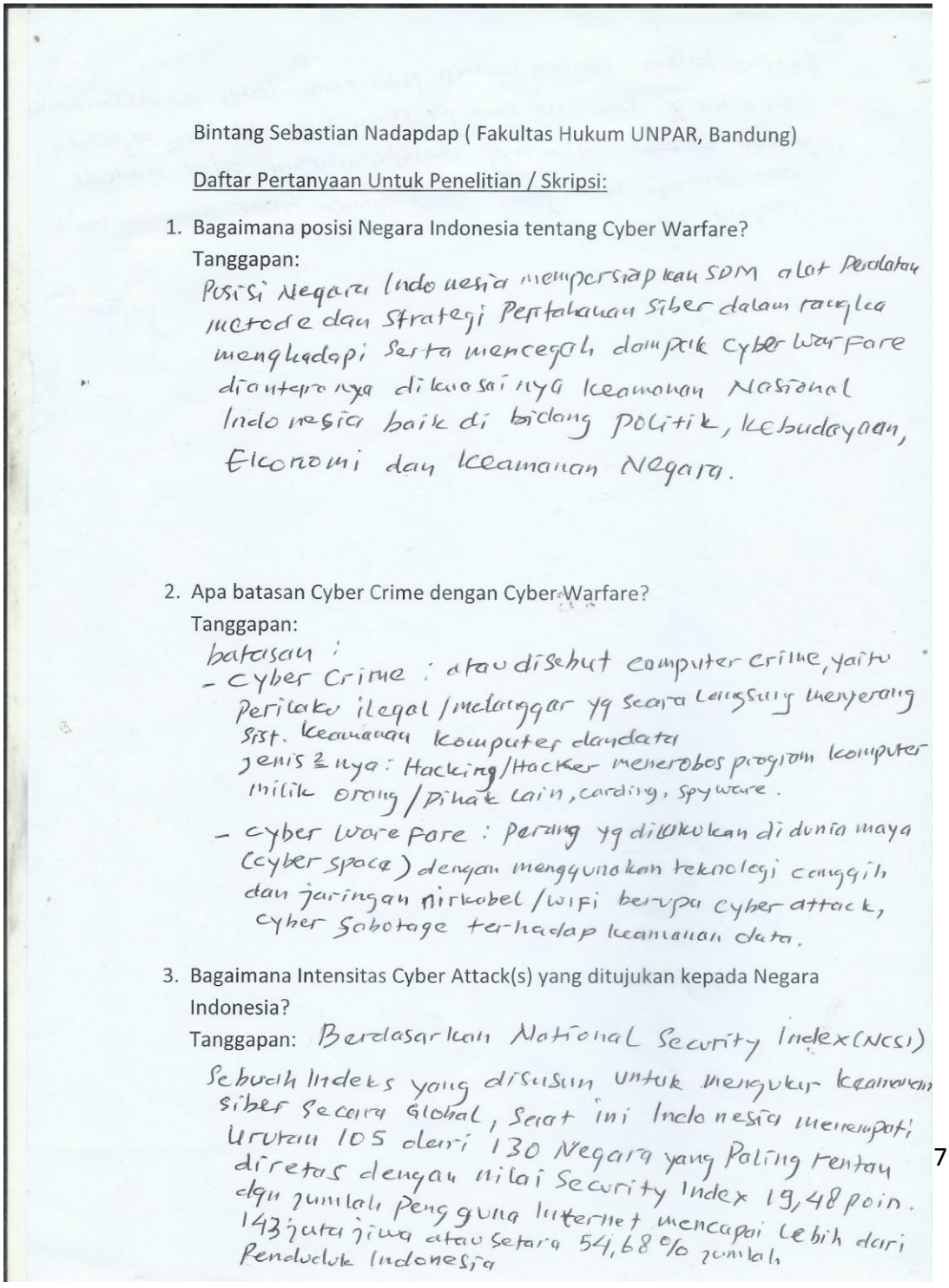
Murdiyono
Kolonel Chb NRP.1900025840764

Tembusan :

- Kapusdatin Kemhan.

Jln. RS. Fatmawati No.1 Pondok Labu Jak - Sel 12450 Telp. 7513010, 7690009, 7657008 Fax. 7504756

Lampiran II (Hasil Penelitian di Pusat Data dan Informasi Kementerian Pertahanan 1)



Bintang Sebastian Nadapdap (Fakultas Hukum UNPAR, Bandung)

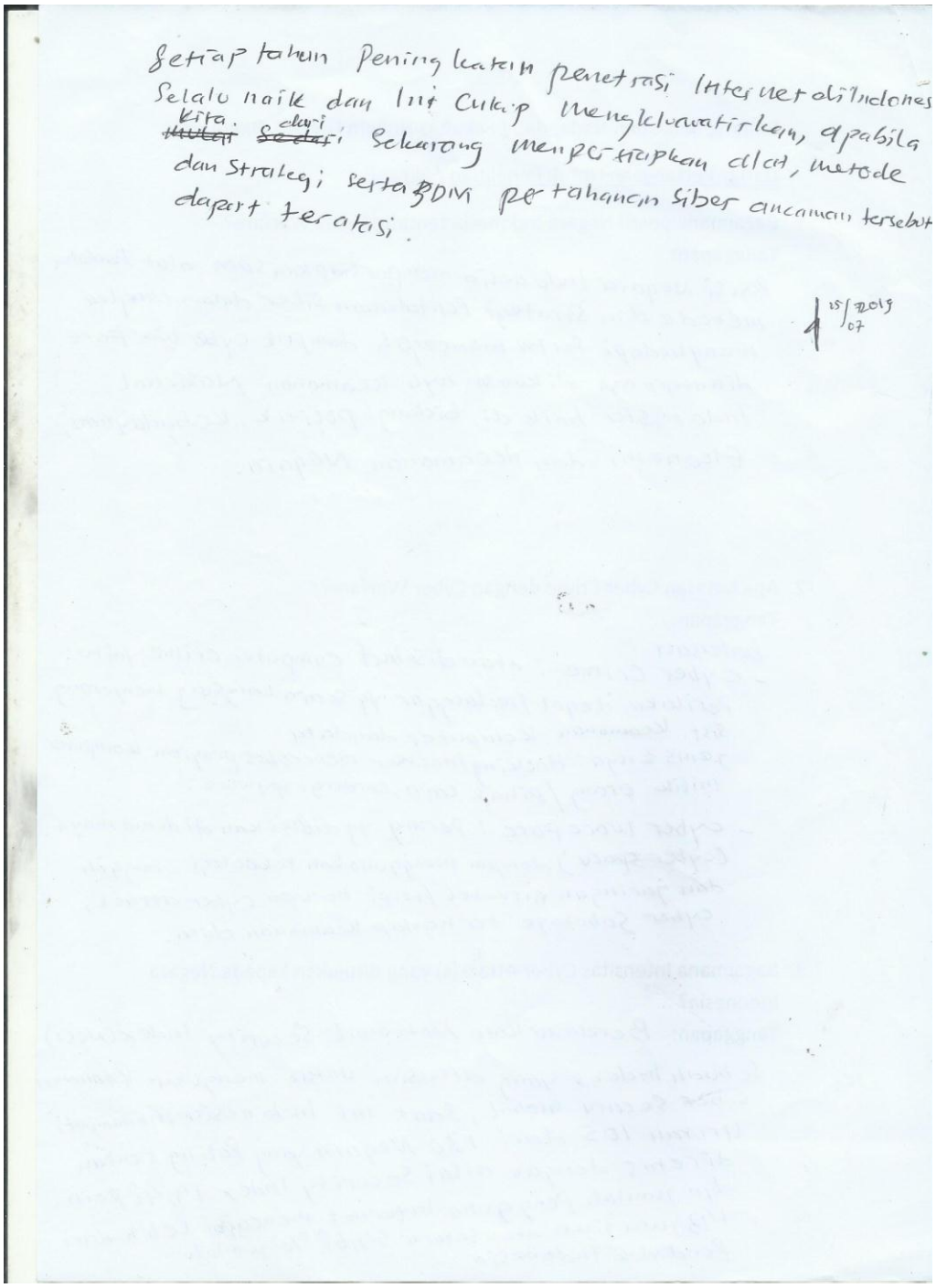
Daftar Pertanyaan Untuk Penelitian / Skripsi:

1. Bagaimana posisi Negara Indonesia tentang Cyber Warfare?
   Tanggapan:
   Posisi Negara Indonesia mempersiapkan SDM alat Peralatan metode dan Strategi Pertahanan Siber dalam rangka menghadapi serta mencegah dampak cyber warfare diantaranya dikarenakan Keamanan Nasional Indonesia baik di bidang politik, kebudayaan, Ekonomi dan keamanan Negara.

2. Apa batasan Cyber Crime dengan Cyber Warfare?
   Tanggapan:
   batasan :
   - cyber crime : atau disebut computer crime, yaitu perilaku ilegal / melanggar yg secara langsung menyerang sist. keamanan komputer dan data
     jenis2nya : Hacking / Hacker menerobos program komputer milik orang / pihak lain, carding, spyware.
   - cyber warefare : perang yg dilakukan di dunia maya (cyber space) dengan menggunakan teknologi canggih dan jaringan nirkabel / wifi berupa cyber attack, cyber sabotage terhadap keamanan data.

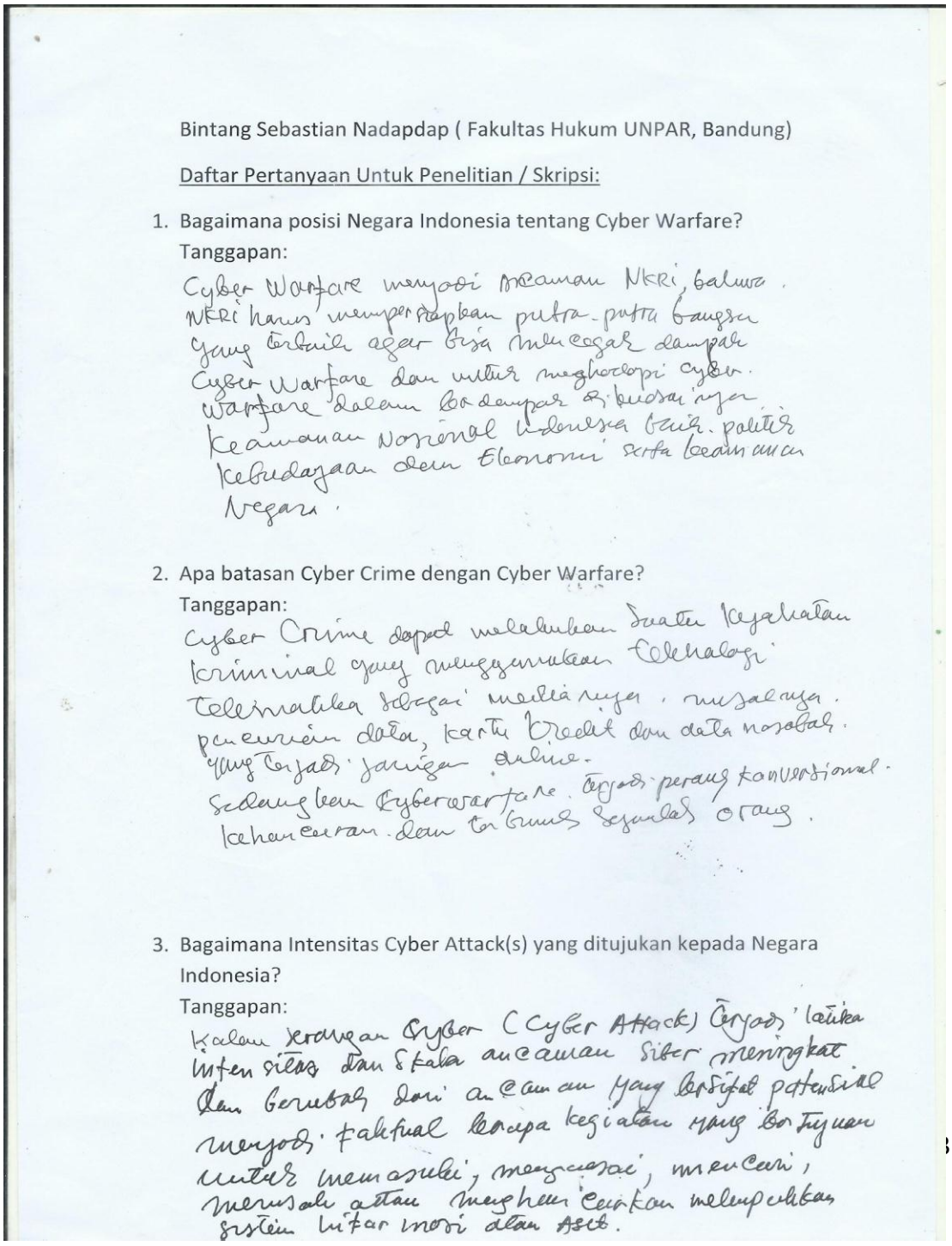
3. Bagaimana Intensitas Cyber Attack(s) yang ditujukan kepada Negara Indonesia?
   Tanggapan: Berdasarkan National Security Index (NCSI)
   Sebuah Indeks yang disusun untuk mengukur keamanan siber secara Global, Saat ini Indonesia menempati urutan 105 dari 130 Negara yang Paling rentan diretas dengan nilai Security Index 19,48 poin. dgn jumlah pengguna internet mencapai lebih dari 143 juta jiwa atau setara 54,68 % jumlah Penduduk Indonesia

Lampiran III (Hasil Penelitian di Pusat Data dan Informasi Kementerian Pertahanan 2)


Setiap tahun Peningkatan penetrasi Internet di Indonesia Selalu naik dan ini Cukup mengkhawatirkan, apabila ~~Hacker~~ ~~Serangan~~ dari kita. Sekarang mempergunakan alat, metode dan Strategi serta SDM pertahanan siber ancaman tersebut dapat teratasi.

15/12/2019
07

Lampiran IV (Hasil Penelitian di Pusat Data dan Informasi Kementerian Pertahanan 3)



Bintang Sebastian Nadapdap (Fakultas Hukum UNPAR, Bandung)

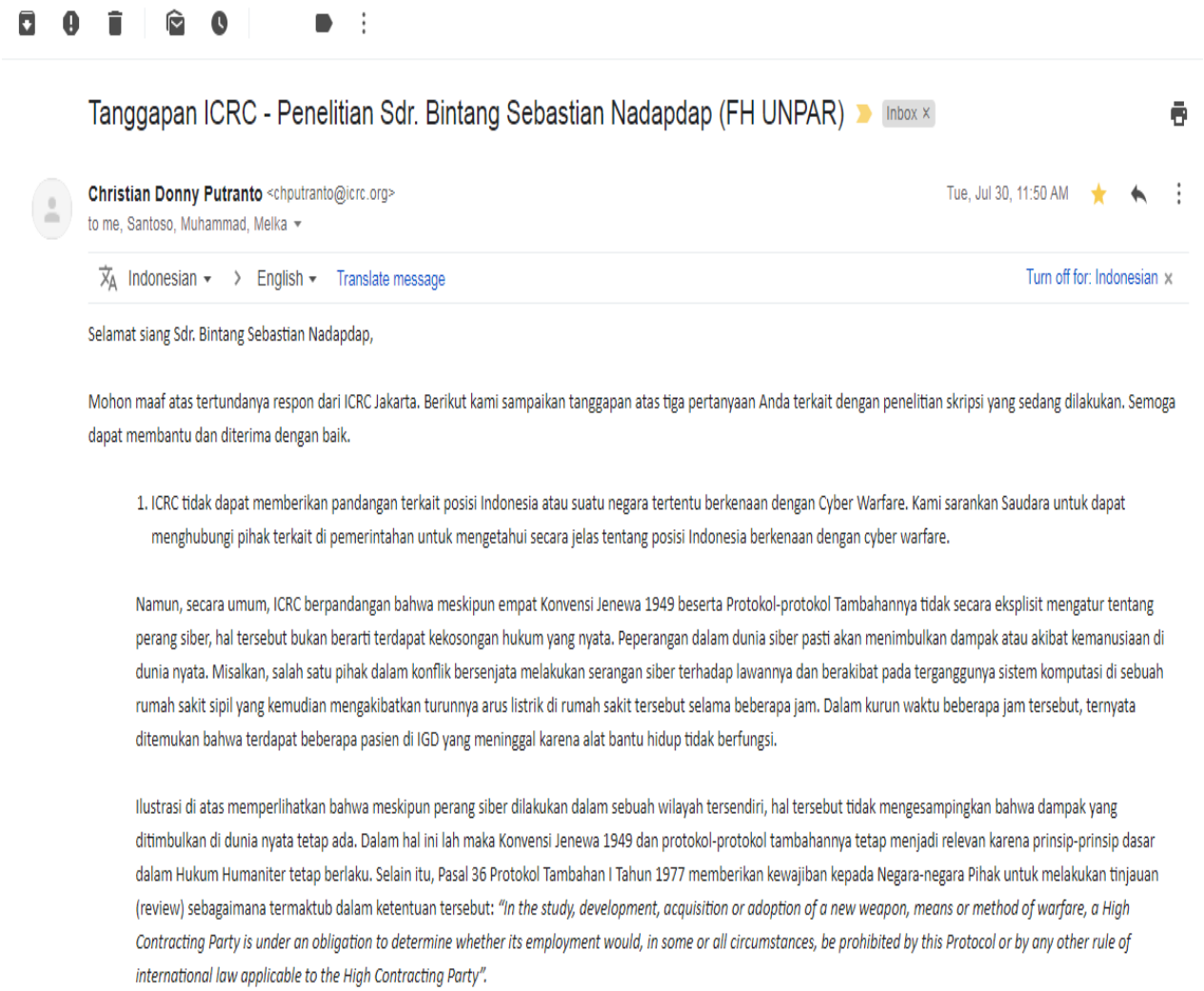
Daftar Pertanyaan Untuk Penelitian / Skripsi:

1. Bagaimana posisi Negara Indonesia tentang Cyber Warfare?
   Tanggapan:
   Cyber Warfare menjadi ancaman NKRI, bahwa NKRI harus mempersiapkan putra-putra bangsa yang terbaik agar bisa mencegah dampak Cyber Warfare dan untuk meghadapi cyber Warfare dalam berdampak signifikan pada Keamanan Nasional Indonesia baik politik kebudayaan dan Ekonomi serta keamanan Negara.

2. Apa batasan Cyber Crime dengan Cyber Warfare?
   Tanggapan:
   Cyber Crime dapat melakukan suatu kejahatan kriminal yang menggunakan teknologi telekomunikasi sebagai media nya, misalnya pencurian data, kartu kredit dan data nasabah yang terjadi jaringan online.
   sedangkan Cyberwarfare terjadi perang konvensional kekerasan dan terbuka sesama orang.

3. Bagaimana Intensitas Cyber Attack(s) yang ditujukan kepada Negara Indonesia?
   Tanggapan:
   Dalam serangan Cyber (Cyber Attack) terjadi' apabila intensitas dan skala ancaman siber meningkat dan berubah dari ancaman yang bersifat potensial menjadi faktual berupa kegiatan yang bertujuan untuk memasuki, mengawasi, mencari, merusak atau menghancurkan melumpuhkan sistem lintas moda dan aset.

Lampiran V (Korespondensi via *e-mail* dengan Internasional Committee of the Red Cross di Jakarta 1)



Tanggapan ICRC - Penelitian Sdr. Bintang Sebastian Nadapdap (FH UNPAR) Inbox ×

Christian Donny Putranto <chputranto@icrc.org> Tue, Jul 30, 11:50 AM

to me, Santoso, Muhammad, Melka

Indonesian › English Translate message Turn off for: Indonesian ×

Selamat siang Sdr. Bintang Sebastian Nadapdap,

Mohon maaf atas tertundanya respon dari ICRC Jakarta. Berikut kami sampaikan tanggapan atas tiga pertanyaan Anda terkait dengan penelitian skripsi yang sedang dilakukan. Semoga dapat membantu dan diterima dengan baik.

1. ICRC tidak dapat memberikan pandangan terkait posisi Indonesia atau suatu negara tertentu berkenaan dengan Cyber Warfare. Kami sarankan Saudara untuk dapat menghubungi pihak terkait di pemerintahan untuk mengetahui secara jelas tentang posisi Indonesia berkenaan dengan cyber warfare.

Namun, secara umum, ICRC berpandangan bahwa meskipun empat Konvensi Jenewa 1949 beserta Protokol-protokol Tambahannya tidak secara eksplisit mengatur tentang perang siber, hal tersebut bukan berarti terdapat kekosongan hukum yang nyata. Peperangan dalam dunia siber pasti akan menimbulkan dampak atau akibat kemanusiaan di dunia nyata. Misalkan, salah satu pihak dalam konflik bersenjata melakukan serangan siber terhadap lawannya dan berakibat pada terganggunya sistem komputasi di sebuah rumah sakit sipil yang kemudian mengakibatkan turunnya arus listrik di rumah sakit tersebut selama beberapa jam. Dalam kurun waktu beberapa jam tersebut, ternyata ditemukan bahwa terdapat beberapa pasien di IGD yang meninggal karena alat bantu hidup tidak berfungsi.

Ilustrasi di atas memperlihatkan bahwa meskipun perang siber dilakukan dalam sebuah wilayah tersendiri, hal tersebut tidak mengesampingkan bahwa dampak yang ditimbulkan di dunia nyata tetap ada. Dalam hal ini lah maka Konvensi Jenewa 1949 dan protokol-protokol tambahannya tetap menjadi relevan karena prinsip-prinsip dasar dalam Hukum Humaniter tetap berlaku. Selain itu, Pasal 36 Protokol Tambahan I Tahun 1977 memberikan kewajiban kepada Negara-negara Pihak untuk melakukan tinjauan (review) sebagaimana termaktub dalam ketentuan tersebut: *"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party".*

Lampiran VI (Korespondensi via *e-mail* dengan Internasional Committee of the Red Cross di Jakarta 2)

2. Istilah ***cyber crimes*** tidak didefinisikan secara spesifik, baik oleh instrumen hukum internasional maupun hukum nasional Indonesia. Sebagai contoh, *The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* mengkategorikan cyber crime dalam arti sempit (sebagai kejahatan yang menargetkan sistem computer) dan arti luas (sebagai segala tindak pidana yang melibatkan sistem ataupun jaringan computer). Begitu pula *Convention on Cybercrimes 2001* yang mengkategorikan beberapa jenis kejahatan siber, tetapi tidak memberikan definisi khusus. Dalam konteks hukum pidana Indonesia, kejahatan siber dapat termasuk dalam kategori tindak pidana konvensional yang diatur di dalam KUHP namun menggunakan sistem computer sebagai sarananya, tindak pidana dalam UU No. 3 tahun 2011 tentang Transfer Dana, tindak pidana pencucian uang dalam UU No. 8 tahun 2010 tentang Pencegahan dan Pemberantasan TPPU, serta tindak pidana dalam UU No. 19 tahun 2016 (UU ITE).

Sementara itu, istilah ***cyber warfare*** juga belum diatur definisi maupun unsurnya dalam instrumen hukum baik internasional maupun nasional. Sumber yang paling sering digunakan sebagai referensi untuk pembahasan mengenai cyber warfare adalah suatu studi yang diadakan oleh sekelompok ahli internasional yang bekerjasama dengan NATO bernama **Tallinn Manual** (dapat diakses dari https://ccdcoe.org/research/tallinn-manual/). Maka dari itu, mengingat kurangnya instrumen hukum yang dapat dijadikan dasar pertimbangan, sulit untuk menentukan batasan definisi dan unsur antara cyber crime dengan cyber warfare.

Sebagai tambahan, *cyber warfare* belum tentu dapat dianggap sebagai *cyber crime*. Begitu pula sebaliknya, cyber crime belum tentu terkait dengan *cyber warfare*. Lalu, sebuah tindakan melalui dunia siber yang dilakukan di negara A dan menimbulkan dampak di negara B perlu juga menjadi perhatian ketika melakukan analisis hukum terhadapnya.

3. Jika melihat studi yang dituangkan dalam Tallinn Manual, masyarakat internasional memandang perlunya pengertian yang jelas dan pengaturan hukum mengenai *nature* dari cyber warfare karena hal tersebut akan menentukan pihak yang terlibat, cara melakukan, alat yang digunakan, serta hal-hal yang harus dilindungi dalam IHL (baca lebih lanjut posisi ICRC terkait cyber warfare dan IHL di https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf).

Terima kasih banyak atas perhatiannya.

Salam,

Christian Donny Putranto
Legal Adviser
International Committee of the Red Cross (ICRC)
Regional Delegation to Indonesia and Timor-Leste
Jalan Iskandarsyah I No. 14, Kebayoran Baru
Jakarta 12160 – Indonesia