Received 1 September 2014; revised 30 December 2014; accepted 1 January 2015.
Date of publication 8 January 2015; date of current version 26 February 2016.

Digital Object Identifier 10.1109/TETC.2015.2389661

An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements

YUDHISTIRA NUGRAHA[1], (Student Member, IEEE), IAN BROWN[2], AND ASHWIN SASONGKO SASTROSUBROTO[3]

[1]Centre for Doctoral Training in Cyber Security, Department of Computer Science, University of Oxford, Oxford OX1 3QD, U.K.
[2]Oxford Internet Institute, Oxford OX1 3JS, U.K.
[3]Indonesian Institute of Sciences, Bandung 40135, Indonesia

CORRESPONDING AUTHOR: Y. NUGRAHA (yudhistira.nugraha@cs.ox.ac.uk)

This work was supported in part by the Indonesian Ministry of Communications and Information Technology under the Directorate of Information Security and the Agency for Research and Human Resource Development, and the first author was supported in part by the Indonesia Endowment Fund for Education Scholarship.

ABSTRACT Edward Snowden's revelations of the extensive global communications surveillance activities of foreign intelligence services have led countries such as Indonesia to take concrete steps to enhance protective information security for classified data and communications. This paper develops the wideband Delphi method to study the Indonesian Government's requirements for cyber-defence in response to reported secret intelligence collection by the Australian Signals Directorate. It provides a clearer understanding of the issues that influence Indonesian policymakers' views on the mitigation of foreign surveillance. We developed and conducted an adaptive wideband Delphi study with senior Indonesian officials, with group discussions and individual sessions to explore how to mitigate the surveillance activities of the Five Eyes (the U.S.–U.K.–Canada–Australia–New Zealand) intelligence alliance. We used the U.S. National Security Agency framework of the three elements of defence in depth (people, operations, and technology), in combination with governance and legal remedies, as an analytical framework. We identified twenty-five mitigation controls to deal with the priority concerns of policymakers, which were divided into a five-defence in depth elements. We discuss the key requirements for protecting against foreign surveillance to be taken into account in state cyber-defence frameworks and suggest effective mitigation controls for safeguarding and protecting states' national interests.

INDEX TERMS State self-defence, defence in depth, adaptive wideband Delphi, foreign surveillance, national interests, information security, requirements.

I. INTRODUCTION

Edward Snowden's revelations have created unprecedented public awareness of the global communications surveillance practices of the five-nation UKUSA alliance (the U.S.-U.K.-Canada-Australia-New Zealand) [8]. Other sovereign states are responding by developing their capacity to protect classified information, as well as to conduct surveillance.

Factors found to affect state perceptions of cyber-defence needs have been explored in several studies. [24] highlights the need for a state self-defence framework to deal with threats and attacks in cyberspace such as distribution of malicious software, unauthorised remote intrusions, and Denial of Service attacks. In addition, the U.S. NSA considers five categories of attacks: passive, active, close-in, insider, and distribution attacks [2]. These categories of attacks can seriously harm an asset in relation to information security properties such as confidentiality, integrity, and availability.

Several recent attempts have been made to protect and safeguard classified information against NSA surveillance programs such as PRISM, Tempora, Upstream, Phone Collection, Xkeyscore, and Stateroom [5], [7], [12], [15]. It is difficult to detect and avoid these type of attacks. Therefore, we have considered reasonable efforts to mitigate global communications surveillance activities through developing effective controls as state cyber-defence requirements.

A number of researchers have suggested that local data clouds, data protection laws, decentralised Internet services, and investment in security professionals and intelligence experts are potential mitigations that should be considered by governments [5], [7], [12], [15].

The research to date has tended to focus on anticipatory self-defence in cyberspace against active cyber-attacks [16], rather than passive attacks such as surveillance, wiretapping and Internet traffic analysis. However, recent studies explored requirements from the Brazilian and German governments against such attacks [5], [21]. These governments have been leading critics of the Five Eyes' activities.

This study investigates the Indonesian government's requirements for state self-defence in response to the case of Australian surveillance of Indonesia. These are analysed in a framework which considers five primary elements - people, operations, technology, governance, and legal remedies.

Indonesia is an interesting case study as a non-aligned, large emerging economy. A quarter of Indonesia's population is currently online with GDP around IDR 9.084 trillion (around USD 753.99 billion) [40]. However, the number is increasing rapidly. According to the Indonesian Internet Service Provider Association (APJII), the number of Indonesian Internet users will increase from 71.19 million in 2013 to 139 million by 2015 [41].

We investigated these requirements using an Adaptive Wideband Delphi Study to gather information from key national stakeholders. This was based on the Wideband Delphi method, in combination with the Delphi study developed at RAND Corporation [6], [11], [13].

We identified twenty-five key requirements from all panellists for state self-defence, in the five-defence in depth themes:

1) *People:*
   a) Awareness, Training and Education;
   b) Information Security Commitments;
   c) Non-Disclosure Agreements;
   d) Proof of Security Clearance;
   e) Local Experts Requirement.
2) *Operations:*
   a) Trustworthy Systems Certification;
   b) Registration of Authorised Software;
   c) Registration of Authorised Hardware;
   d) Incident Response Management;
   e) Security Continuous Monitoring.
3) *Technology:*
   a) System and Communications Protection;
   b) National Cryptographic Standards;
   c) Local Applications Platform;
   d) National Infrastructures Platform;
   e) Control of International Traffic.
4) *Governance:*
   a) Independent Review Agency;
   b) Risk Management Process;
   c) Information Security Baseline;
   d) Impact of Potential Threats;
   e) Domestic Hosting and Domains.
5) *Legal Remedies:*
   a) Information Security Agreement;
   b) Regulation of Data Protection;
   c) Data Centre Localisation;
   d) Lawful Interception Capability;
   e) Code of Ethics and Conduct in Bilateral Cooperation Treaties.

Indonesian policymakers' preferences for state self-defence requirements to mitigate foreign surveillance often matched the security control sets from ISO/IEC 27001 Requirements - Information Security Management System [14], NIST Special Publication 800-53 on Security and Privacy Controls [27], and 20 Critical Security Controls [29].

Every state must build their own state cyber defence requirements against foreign intelligence services. Therefore, such a model can be built on by less developed countries, which have fewer resources to address the technical complexity, policies, and activities needed to build confidence and manage vulnerabilities and threats inherent in cyberspace.

The remainder of this article is structured as follows: Section II describes background and related work to position contributions of this work. Section III explains our research methodology. Section IV provides a analytical framework for state self-defence requirements. Section V presents the results, followed by an analysis and discussion of their limitations. Finally, Section VI concludes the paper.

II. BACKGROUND AND RELATED WORK

In this section we provide a brief review of a Delphi approach to develop an understanding of the requirements for state self-defence against communications surveillance by extremely sophisticated opponents, using Indonesia as a case study. This effort can illuminate possible solutions for other countries to strengthen national security and protect against foreign intelligence services in general. We then review the requirements for state self-defence in cyberspace against active and passive attacks. This section also includes a detailed description of the cyber defence framework that we used in this study.

A. DELPHI APPROACH TO DEVELOP STRATEGY

The Delphi method was first developed at RAND Corporation in the 1950s as part of a military defence project [11], [25]. This method moderates the influence of dominant individuals and follows a rigorous sequence of steps for decision making in the context of policy formulation [11]. All features of the Delphi procedures such as anonymity, iteration and controlled feedback, and statistical group response are used to elicit and refine group estimation and consensus [11], [25]. It avoids direct conflict of the participating experts due to the absence of face-to-face communication [28].

A variety of adapted Delphi methods are widely used to assess specific problems based on a number of situations [28]. For example, if the participants are distributed across

different locations, the experts can participate by connecting via a custom website [18] or email [25].

The wideband Delphi method involves greater interaction and more communication between participants than the classic Delphi approach [33]. Group discussion occurs between rounds in which participants explain their statements and opinions [6]. Potter and Sakry's variant requires further group discussion to revise estimates and achieve consensus. An iterative process terminates when no participants want to revise the collective estimation [32].

Traditional Delphi studies avoid face-to-face meetings in order to elicit genuine opinions and anonymous input. However, the wideband Delphi estimation panel discussion stage can clarify the major issues when ''judgmental information is indispensable'' [28], and is used to seek all requirements as ''informed judgement'' [39].

However, there are certain problems with the use of Delphi. There is less control over the period from securing work schedules of policymakers and experts when conducting face-to-face meetings. Every country has a different culture and work behaviour. In addition, policymakers and experts must consider the context of policy formulation is of paramount importance. Therefore, researchers need to give potential participants a clear understanding of the problem description and the Delphi steps before the study begins. At least one researcher should be well-known by potential participations and have contacts with the participating policymakers and experts.

Due to the uncertainty inherent in the question with specific culture and work behaviour of Indonesia, we created an adaptive Delphi method based on the Delphi technique and the wideband Delphi approach. This method is one of the more practical ways of eliciting requirements for state self-defence by using appropriate features of Delphi such as anonymous individual feedback, controlled feedback, group responses with face to face meetings for eliciting and refining the converged requirements. The final step of this method is to obtain reviews and an initial approval from the policymakers.

B. RELATED WORK

There is not yet an international consensus on the definition of state self-defence in cyberspace. Article 51 of the United Nations Charter indicates that every state has the right of self-defence and collective self-defence against attacks [17]. The issue of how to protect a state from such cyber-attacks including global communications surveillance has not been resolved. Thus, in this article, state self-defence refers to continuous efforts to safeguard and protect state sovereignty, national territory, and the nation's safety against all type of threats.[1]

[1]The definition of state self-defence is adopted from the Indonesian Law Number 3 of 2002 on State Defence, in terms of how to protect a state against cyber threats such as foreign intelligence services, industrial espionage, organised cybercrime groups and non-state actors.

1) SELF DEFENCE AGAINST ACTIVE ATTACKS

Many countries regard cyberspace as a new theatre of war [13]. As a result, nations need to look beyond article 51 of the UN Charter. It has been suggested that it is important to maintain the rights of state self-defence as applied to threats in cyberspace, as on other domains such as land, sea, and air [23].

Kesan and Hayes analyse state self-defence rights to protect critical national infrastructure (CNI) located within their jurisdiction [24]. They draw on extensive range of sources to assess whether ''mitigative counterstriking capabilities'' can be implemented effectively in cyberspace for protecting CNI. They propose a legal framework that would allow the use of active self-defence in cyberspace in order to reduce and mitigate risks from the current and immediate threats against CNI.

Todd investigated the control of armed attacks in cyberspace [35]. He argues that a state still cannot legitimately act in self-defence without violating another state's sovereignty. He suggests that under the current law, the victim state should send requests to another country as well as cooperate with other countries in gathering information, because cyber attacks that come from another country may have been carried out by a 'hopping' route-pattern through several other countries.

Graham points out that the requirements such as necessity and proportionality limit the use of self-defence techniques. Therefore, policymakers need to pay attention to the implementation of self-defence measures from both legal and policy perspectives [19].

This view is supported by Caulkins, who examined developing proactive tools to combat new and emerging threats in cyberspace [10]. He made a set of strategic recommendations for establishing a proactive self-defence policy: ratify cyber-related legislation, develop a robust architecture for proactive cyber security, design disruption tolerant networks (DTN), conduct security training and education in the cyber realm, and to provide funding for cyber activities. He suggests the use of both reactive and proactive tools so that the governments have capabilities to protect CNI against cyber-attacks.

In the same vein, Guiora proposed a new approach to preventive self-defence against non-state actors [20]. He considers anticipatory operational measures that can be implemented against cyber threats as well as combating future threats. It offers some important insight into the requirements for state self-defence. However, further work would be needed to develop a self-defence framework.

Gill and Paul were more concerned with legal frameworks governing the exercise of anticipatory self-defence [16]. They argue that anticipatory self-defence may be carried out in response to an imminent cyber armed attack irrespective of whether the attack is performed by a state, or non-state actors, with or without much greater state involvement. They establish a framework for the right of self-defence within the

current provisions of the UN Charter and customary international law. The findings can be used in state self-defence to identify, which requirements should be addressed to meet national interests.

2) SELF DEFENCE AGAINST PASSIVE ATTACKS

Following the leaked documents supplied by Edward Snowden, a considerable amount of literature has been published on state responses to communications surveillance activities. Some requirements for state self-defence against threats of global communications surveillance have been identified.

For example, standard cryptographic protocols can be a feasible control against 'built-in wiretapping capabilities' for preserving privacy [12]. In the same vein, it seems clear that centralised Internet services play an important role in supporting the current surveillance practices. It has then been proposed that the development of global Internet services such as cloud services should be based on open-source platforms and decentralised services-configuration [12].

Similarly, Brown elaborated requirements in relation to privacy-protective standards for surveillance, including data sharing privacy agreements, state-state negotiations over intelligence sharing, and human rights protections [7].

Moreover, some policy practices from the Brazilian government and the German government have been outlined by Bauman, et al. such as the creation of local data clouds, development of surveillance capabilities, investment in security professionals and intelligence experts, and in the Brazilian case, attempts to develop domestic content as well as international Internet connectivity beyond the scope of the U.S. Internet infrastructure [5].

In addition, it has been shown that effective legal frameworks must be in place to regulate state access to data so that individual citizens can trust government [34].

3) FEATURES OF A STATE SELF DEFENCE FRAMEWORK

It is up to each state to determine to what extent it will protect national security and privacy in cyberspace and how to pursue this end. This study focuses on global communications surveillance as a passive attack that is operated by the Five Eyes nations' signals intelligence (SIGINT) operational platforms [3]. The NSA considers passive attacks as a class which includes monitoring of communications, decrypting encrypted information, Internet traffic analysis, and capture of authentication information that can lead to disclosure of information without user consent [2].

The ITU Plenipotentiary Conference in Resolution 130 stated that every state has sovereign rights for the purpose of national defence, national security, content, and cybercrime [36]. In other words, a state is responsible for developing a set of requirements for state self-defence based on the state's national interests. However, developing the requirements for state self-defence to mitigate foreign surveillance activities is likely to be a complex process that requires a balanced perspective from different areas of expertise.

States can manage and mitigate threats and risks from communications surveillance through the implementation of a defence in depth strategy. The NSA Framework identifies three primary elements in achieving information assurance, which are people, operations and technology [1]. The Trusted Information Sharing Network (TISN) introduced another additional element, which is governance in order to oversee the implementation of people, operations, and technology [26]. The Lukasik-Goodman-Rutkowski (LGR) framework defines mandatory cyber security activities, both legal and other actions such as ''measures for protection, measures for threat detection, measures for thwarting, investigation and measure initiation, and legal remedies'' [30]. The ITU Global Cybersecurity Agenda (GCA) also established a framework within the development of national cyber security strategy into five pillars, which are (1) legal measures, (2) technical and procedural measures, (3) organisational structures, (4) capacity building, and (5) international cooperation [37].

This paper used the integration of the five primary elements, which are people, operations, technology, governance, and legal remedies.

III. RESEARCH DESIGN

We used an adaptive wideband Delphi study to enable the surveying of multiple panellists from key national Indonesian stakeholders through face-to-face qualitative stages such as panel discussions to clarify the major issues of global communications surveillance, along with anonymous individual feedback to gather genuine requirements to mitigate such risks.

Since the motivation and experience of the participants directly affects the quality of findings, particular attention was paid to the selection of panellists. To achieve a wide range of stakeholders, four relevant categories of panellists, with valuable knowledge about requirements for state self-defence, were chosen: government officials and military officers, academics, industries and practitioners.

Three industry panellists were from telecommunications providers whose network infrastructure have been reported to be compromised according to Edward Snowden's revelations. The rest of the industry panellists come from Indonesia's Internet Service Provider Association. Practitioners were consultants who are working in the field of information security.

Panellists were chosen according the following the selection criteria: 1) work experience and background, 2) a self-critical attitude, 3) involvement in policy-making process, and 4) a visible interest in the research topic, in order to achieve meaningful results and keep the failure rate as low as possible [22].

The panels were formed based on expertise and background experience. We invited 20 panellists[2] consisting of eight government officials; four academics; four panellists

[2]The information given will be anonymised and for additional information, please contact the corresponding author.

from telecommunication operators and the Internet Service Provider Association; and four panellists from information security practitioners. In this case, the size of the panel would not have an effect on the findings; thus there is no requirement to meet the size of a panel of experts [31]. However, it is important to consider other characteristics of panels to have qualified and appropriate panellists to discuss the major issues and propose the solutions.

Based on the wideband Delphi steps, we conducted three face to face meetings as follows:

1) Kick-off meeting during first round.
2) Panel discussion during second round.
   a) Panel 1(Government officials and Military Officers).
   b) Panel 2 (Academics).
   c) Panel 3 (Industries).
   d) Panel 4 (Practitioners).
3) Final meeting during third round.

We also adapted the features of the Delphi approach to make separate panel discussions for the second round to gather specific group responses, because these panels perhaps would have different positions that related to participants' affiliations.

We then further asked each panel to identify specific and reasonable requirements. Finally, consolidated requirements from each panel were summarised and combined to obtain convergence requirements.

This design also allows making the comparison of different frames of mind from panellists. We asked each panellist respectively to describe their opinions in relation to state self-defence requirements. We then asked each panel to make consolidated requirements.

A. DATA COLLECTION METHOD

Data collection took place in seven stages as follows, as shown in figure 1:

1) Panel selections;
2) Kick-off meeting;
3) First individual feedback;
4) Panel discussion;
5) Convergence results;
6) Second individual feedback;
7) Consolidated meeting.

In the first step, we selected a moderator and formed four panels of experts with three to seven members [31]. We also asked the policymakers to advise on the potential panellists. We then selected the panellists based on their confirmation.

The second step was the kick-off meeting where we delivered a presentation and provided related documents to the panellists. We then asked all panellists to create a general list of requirements and discuss the major issues that related to cyber defence requirements. We asked each panellist to give their opinions individually, followed by comments and discussions on a general list of requirements.

For the third step, after the meeting, we asked each panellist to review and revise the requirements based on the results. Then, each panellist sent an individual anonymous feedback statement for the requirements for state self-defence by

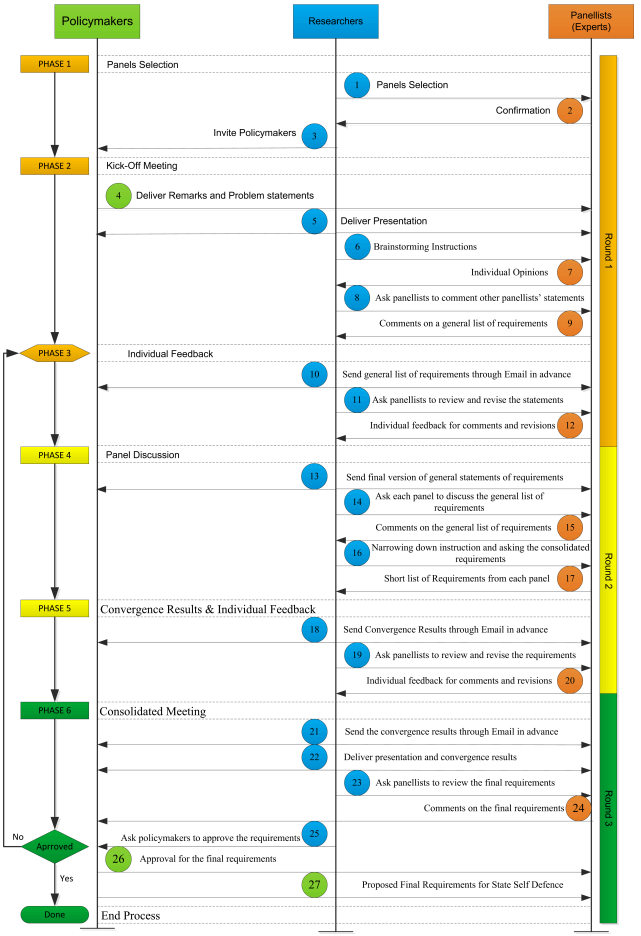

FIGURE 1. Adaptive wideband delphi framework.

e-mail [25]. In this case, only the researchers know the individual feedbacks behind the investigation of cyber defence requirements [38].

The fourth step was the panel discussion, in which each panel discussed a general list of requirements and stated requirements for state self-defence derived from the previous steps. This second round typically results in a narrowing of the list of requirements through group discussion, pointing to some clarification and asking each panellist to sharpen their requirements specifically in relation to mitigation of foreign surveillance.

In the fifth step, we summarised the results, and asked each panellist to individually review and revise the requirements in the form of anonymous individual feedback. All individual feedback was conducted anonymously through email, and only the researchers knew who proposed and generated those requirements.

The final step was a meeting to review the requirements for state self-defence with all panels along with senior Indonesian policymakers. This third round summarised a list of requirements to be reviewed, and was approved by Indonesian policymakers.

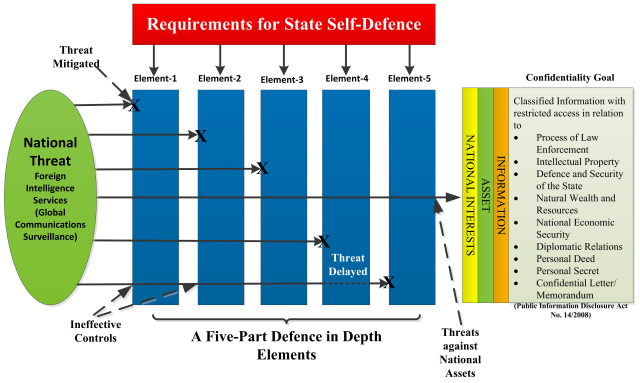

FIGURE 2. **Mitigation approach for foreign surveillance, [modified from [4]].**

IV. ANALYTICAL FRAMEWORK

We adopted the general defence in depth schema in [4] with modifications in relation to mitigation approaches for passive threats and attacks such as foreign surveillance activities, as shown in figure 2. The study defined fundamental requirements as mitigation controls for each of the five-part defence in depth elements based on states' national interests. The multiple elements of defence help ensure that the likelihood can be mitigated or at least the attacks slowed down [4].

TABLE 1. **Threat model for communications surveillance.**

State Self Defence	Information Asset Risk
Information Asset	Classified Information according to - Public Information Disclosure Act No. 14/2008 - National Intelligence Act No 17/2011)
The Area of Concern	Critical National Infrastructure
Actor	**Foreign Intelligence Services** In this case, the five nations UKUSA Alliance (1) US — NSA (2) UK — GCHQ (3) Canada — CSEC (4) Australia — ASD (5) New Zealand — GCSB
Means	**Communications Surveillance :** ECHELON PRISM TEMPORA FAIRVIEW XKEYSCORE STATEROOM
Motivate	**Deliberate**
Outcome	**Disclosure**
Security Requirement	**Confidentiality**
Probability	**High**
Consequences	(1) It may disturb the protection of the right to intellectual property. (2) It may be hazardous to the defence and security of the state. (3) It could reveal the natural wealth of Indonesia. (4) It may be harmful to the national economic security. (5) It may be harmful to diplomatic relations. (6) It may reveal personal data and privacy.
Impact Area	State Security Privacy
Mitigation Controls	People Operations Technology Governance Legal Remedies

We then examine the threats of communications surveillance as a real-life case shown in Table 1. We adopted the table from the OCTAVE Allegro Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [9].

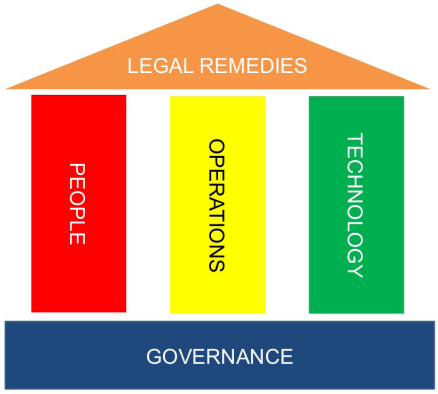

FIGURE 3. **A Five-Defence in Depth Elements.**

TABLE 2. **Defence in depth framework.**

Element	Description
People	The implementation of an information security program begins with top management commitment based on a clear understanding of the perceived threats. Establishment of effective information security policies and procedures must follow, along with a clear understanding of roles and responsibilities; financial resources; training of key personnel; and enforcement of personal accountability. These involve setting up the security personnel and physical security measures to control and monitor access to facilities and critical information [1].
Operations	The operations element focuses on all activities required to maintain an organisation's security stance on a day-to-day basis. These include certification and accreditation, security management, key management, readiness assessments, attack sensing, warning and response and recovery and reconstitution [1].
Technology	A number of technologies are available for implementing information security. To ensure that the right technologies are procured and deployed, an organization should establish effective policies and processes for technology acquisition. These policies and processes should include security policy, information security principles, security architectures and standards, criteria for hardware and software assurance, procurement of hardware and software that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems [1].
Governance	The governance element involves a management framework providing oversight and coordination of people, operations and technology. This include risk management, information security, and policy and compliance management [26].
Legal Remedies	This layer is an umbrella of people, operations, technology and governance. This includes intergovernmental agreements and cooperation, contractual services agreements and federations, tort and indemnification, regulatory and administrative law, and criminal law [30].

We introduced an information assurance model for the requirements of state cyber defence that can help mitigate foreign intelligence surveillance, as shown in figure 3. We then provide details of this framework in Table 2.

Defence against the threat model we provided requires the integration of the five primary elements-people, operations, technology, governance, and legal remedies.

V. RESULTS AND ANALYSIS

This section presents the results of our adaptive wideband Delphi study. We give an overview of the results. We then present analysis and discussion for each element.

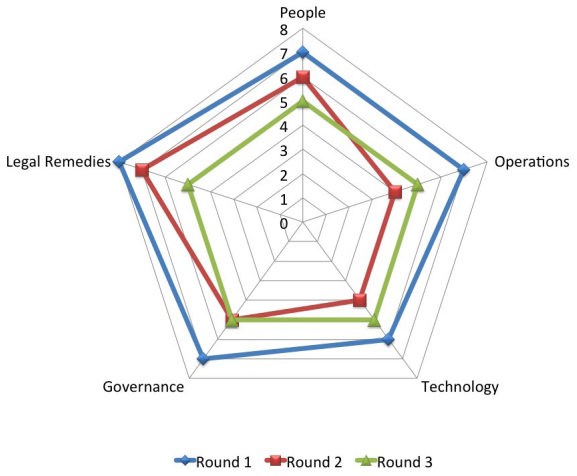

FIGURE 4. Distributed requirements statements for state self defence.

Our participants determined twenty-five primary requirements for state self-defence. Each panellist stated requirements based on their perception of the state's national interests.

Figure 4 shows that the first round identified thirty-five general requirements. The second round, panel discussions, found agreement on twenty-six requirements from each panel. In the third round, the twenty-five requirements were proposed by panellists and reviewed by Indonesian policymakers.

Some considerations that one or two panels assessed to be more worthy of attention were not selected by others. For example, the top-ranked requirements for the government panel were 'security awareness'. Other panels also listed this. However, not all panels selected the same items for requirements. This supports the methodology of eliciting requirements from multiple stakeholders because it enables more comprehensive coverage.

It is difficult to create a list of requirements statements across multiple stakeholder settings. However, the study encouraged each panellist to identify the requirement statements based on their expertise and experiences in order to avoid situational requirements. We then asked panellists to discuss and consolidate the requirements in common as converged requirements.

The major types of selected requirements were almost the same for each round because the levels of consistency on the requirements were moderately strong within the three-round Delphi. We then focused on the set of twenty-five requirements that were proposed by all four panels alongside an initial approval from senior officials.

It is apparent in Table 8 that there are some novel concepts of Indonesian requirements for state self-defence, while other requirements are also addressed in the security control sets in ISO/IEC 27001 [14], NIST Special Publication 800-53 [27], and 20 Critical Security Controls [29].

The list of the twenty-five requirements is a combination statement from all panellists, divided into the five defence in depth elements of People, Operations, Technology, Governance, and Legal Remedies. Each requirement is written as a constraint on how a state might operate for self-defence. In fact, the terminology for this study follows the general format 'The Government of Indonesia must' [4].

A. PEOPLE

In case of the People element, we asked panellists to indicate the requirements that represented the appropriate control for personnel security roles and responsibilities.

In this section, five common requirements are described that are intended to improve the depth of security roles and responsibilities for internal and external stakeholders, by developing security culture and mind-set. The requirements focus on management commitment for information security and personnel security including security awareness.

TABLE 3. Risk and requirement of people element.

Risk	Requirement	Description	Reasonable Effort
Awareness and Skills	Awareness, Training and Education	The Government must provide evidence that all employees receive appropriate security awareness, training and education with regular updates for protecting classified information under the laws.	This requirement helps ensure that effort has been made to develop information security culture and mind-set within the organisation as well as to ensure cyber defence requirements can be fully implemented.
Leadership	Information Security Commitment	The Government must provide evidence that the critical infrastructure owners actively support the implementation of information security policy within the organisation.	This requirement helps ensure that top management demonstrates their commitment to information security policy by establishment of an information security framework.
Rules and Compliance	Non-Disclosure Agreement	The Government must provide evidence that a non-disclosure agreement for protecting classified information is in place and is regularly reviewed.	This requirement helps ensure that the organisation preserves authorised restrictions on information access and disclosure, including means for protecting classified information.
Insider Threat	Proof of Security Clearance	The Government must provide evidence that a set of formal screening process has been established for all employees, contractors and third party users.	This requirement helps ensure that security clearance process must be in place. It should involve personnel security mechanism prior to employment, during employment and termination of employment.
Human Resources	Local Experts Requirement	The Government must provide evidence that critical infrastructure owners shall employ local experts in certain areas.	This requirement helps ensure that reasonable effort has been made to manage serious impacts to state defence and security.

1) RESULTS

We determined the requirements in relation to People as follows:

1) Awareness, Training and Education (ATE);
2) Information Security Commitment (ISC);
3) Non-Disclosure Agreement (NDA);
4) Proof of Security Clearance (PSC);
5) Local Experts Requirement (LER).

We summarise the details of these requirements in Table 3.

2) ANALYSIS AND DISCUSSION

The panellists indicated that the weakest elements are human capacity building in terms of security awareness. Specifically, awareness for those people who have access to the organisation's information assets is the biggest challenge. In response to this, the government should enhance security awareness programs including developing security culture, behaviours and security mind-set.

People factors are an important source of cyber security risks generated by individual employees and contractors, and third party users. In this case the most important risk factor is lack of user awareness. If combined with other risks such as lack of leadership, lack of rules and compliance, insider threats and involvement of foreign experts create the number of potential national threat points of entry. We summarise risk associated with the requirements in Table 3.

It is obvious that some requirements map onto other security standards such as ISO/IEC 27001 [14], NIST SP 800-53 [27] and 20 Critical Security Controls [29]. Most of them cover these requirements except in terms of local experts requirements. A summary of related controls in relation to these requirements is in Table 8.

B. OPERATIONS

For the Operations element, we asked panellists to discuss operational actions to improve the depth of security mechanisms for critical infrastructures. The majority preference was to establish a security incident response team and security continuous monitoring. The other requirements focus on all the activities required to sustain an organisation's security posture on a day-to-day basis, and are used to ensure the continuous security stance of the organisation.

1) RESULTS

We found the requirements in relation to Operations as follows:

1) Trustworthy Systems Certification (TSC);
2) Registration of Authorised Software (RAS);
3) Registration of Authorised Hardware (RAH);
4) Incident Response Management(IRM);
5) Security Continuous Monitoring (SCM).

We summarise the details of these requirements in Table 4.

2) ANALYSIS AND DISCUSSION

It is clear that the policymakers want to build a trusted and resilient cyber environment against threats and attacks in cyberspace through certification and assessment in relation to system components. The preference for state self-defence requirements was evident even though there was a degree of flexibility in relation to the priority requirements in which this should be implemented.

From a cybersecurity risk perspective, lack of security operations are often exploited by adversaries. Examples include installing backdoors in hardware and software. In addition, known weaknesses and zero-day vulnerabilities can be exploited by adversaries. Therefore, the policymakers should make reasonable efforts to assure that the hardware and software must pass the security evaluation and be certified by local authorities.

TABLE 4. Risk and requirement of operations element.

Risk	Requirement	Description	Reasonable Effort
Trusted Electronic System	Trustworthy Systems Certification	The Government must provide evidence that certification of worthiness for electronic systems are in place to any critical information infrastructures.	This requirement helps ensure that all critical information infrastructures must be examined and tested in order to increase reasonable confidence in operations and security.
Software Vulnerabilities	Registration of Authorised Software	The Government must provide evidence that effective registrations of authorised software applications are in place and are maintained to minimise security risk.	This requirement helps ensure that reasonable effort has been made to assure that the software does not contain any malicious code as well as to evaluate zero-day exploits on various software.
Hardware Vulnerabilities	Registration of Authorised Hardware	The Government must provide evidence that effective registrations of authorised hardware are in place and are maintained to minimise security risk.	This requirement helps ensure that all devices in relation to critical information infrastructures have passed the security evaluation and reasonable effort has been made to control surveillance mechanisms built into hardware.
Incident Response	Incident Response Management	The Government must provide evidence that the organisation has the ability to respond to indicators in advance of threats and attacks on any critical information infrastructure.	This requirement helps ensure that response activities are coordinated with related parties and performed based on indicators with established criteria.
Control and Monitoring	Security Continuous Monitoring	The Government must provide effective procedures for security continuous monitoring of unauthorised classified information processing activities.	This requirement helps ensure that classified information is regularly monitored to identify information security events. Vulnerability assessments must be in place for the effectiveness of protective measures.

In this case the most important risk factor is the lack of trustworthy systems used for critical national infrastructure. As a result, if combined with other risks such as zero-day attacks and discontinuous controls and monitoring, it can lead to a period of time in which security breaches and attacks are much more common in critical national infrastructure. We summarise risk associated with the requirements in Table 4.

The findings clearly highlight that the existing security controls mostly cover these selected requirements, except one requirement in relation to Trustworthy Systems Certification. Details of related controls are listed in Table 8.

C. TECHNOLOGY

In this section, we describe five requirements identified by panellists that are intended to improve the depth of technical controls to protect critical information infrastructure.

A variety of perspectives were expressed. The panellists stated it was important to strengthen national capabilities in the development of appropriate technologies to reduce risks related to foreign surveillance. For example, panellists stated that paying attention to security and privacy must be in place to protect and secure the classified information by means of cryptographic controls and utilising national secure networks and devices provided by National Crypto Agency.

1) RESULTS

We found the requirements in relation to Technology as follows:

1) System and Communications Protection (SCP);
2) National Cryptographic Standards (NCS);
3) Local Applications Platform (LAP);
4) National Infrastructures Platform (NIP);
5) Control of International Traffic (CIT).

We then summarised the detailed of these requirements in Table 5.

TABLE 5. Risk and requirement of technology element.

Risk	Requirement	Description	Reasonable Effort
Networks Infrastructure	System and Communications Protection	The Government must provide evidence that access to networks is appropriately controlled and reasonable secured.	This requirement helps ensure that reasonable effort has been made to mitigate the networks be designed wiretap-ready.
Information Architecture	National Cryptographic Standards	The Government must demonstrate compliance with national cryptographic standards to protect security and privacy of classified information.	This requirement helps ensure that reasonable effort has been made to protect classified information related to the state secrets.
Platform	Local Applications Platform	The Government must enforce critical information infrastructure owners to use in-house applications platform to minimise risks of foreign surveillance.	This requirement helps ensure that the organisations utilise local applications platform for data sovereignty as well as to overcome zero-day attacks.
International Backbone Dependencies	National Infrastructures Platform	The Government must enforce critical infrastructure owners to use the national infrastructure platform to minimise risks of foreign surveillance.	This requirement helps ensure that the national infrastructure communications must be utilised in accessing classified information as well as delivering confidential information related to the state secrets.
Information Flows	Control of International Traffic	The Government must provide evidence that information flow to outside jurisdiction is controlled on a regular basis and disseminated to policymakers on a timely basis.	This requirement helps ensure that the government has a means for protecting classified information, which intended to deliver outside the country.

2) ANALYSIS AND DISCUSSION

The panellists were clear about the requirement for the establishment of national capabilities, especially to strengthen critical information infrastructure security and resilience.

In the Indonesian case, attempts to employ national infrastructure such as the construction of a 'Palapa Ring Project', Fibre Optic Backbone Infrastructure as well as to expand national gateway for Internet connectivity within national border are consistent with the idea of safeguarding and protecting state security and privacy against communications surveillance. Indonesia's domestic Internet connectivity is highly dependent on international backbones. Zero-day exploits exist for platforms and reduced control of information flows creates a number of potential national risks against global communications surveillance. In addition, the number of potential threats outside the jurisdiction have grown due to the degree of control over the Internet by the UKUSA alliance. We summarise risk associated with the requirements in Table 5.

Interestingly, the existing standards only cover two of the identified requirements, in relation to system and communication protection, and cryptographic control. The other three requirements seem to be novel requirements for the government in order to mitigate foreign surveillance activities. Related controls are reported in Table 8.

D. GOVERNANCE

We asked panellists to discuss governance frameworks to mitigate foreign surveillance. We identified five governance requirements intended to provide oversight and coordination of people, operations and technology, related to organisational structure, baseline information security implementation, risk management process, determination of threat level, and use of domestic hosting and domain names.

1) RESULTS

We found the requirements in relation to Governance as follows:

1) Agency of Independent Review (AIR);
2) Risk Management Process (RMP);
3) Information Security Baseline (ISB);
4) Impact of Potential Threats (IPT);
5) Domestic Hosting and Domains (DHD).

We summarise the details of these requirements in Table 6.

TABLE 6. Risk and requirement of governance element.

Risk	Requirement	Description	Reasonable Effort
Control Deficiencies	Agency of Independent review	The Government must provide evidence that critical information infrastructures that could directly affect the state security, is subject to reviewed by an agency that is responsible for national security.	This requirement helps ensure that security mechanism reviews are in place to analyse potential threats and impacts. It should include evidence through national information security risk assessment.
Damage and Lost	Risk Management Process	The Government must enforce critical infrastructure owners to apply risk management system for any damage or disadvantages, which may arise.	This requirement helps ensure that risk management processes must be in place and are regularly managed. It should include evidence that national security risk assessment must be in place.
Compliance and Control	Information Security Baseline	The Government must has a written policy for implementation information security baseline within critical infrastructures.	This essential part of this requirement is that the implementation of information security management system must be in place as minimum requirements.
Escalation Process	Impact of Potential Threats	The Government must provide evidence that impact level of potential threats has been established for which type of threats in which contexts must be mitigated and escalated by the critical infrastructure owners.	This requirement helps ensure that vulnerabilities and threats to national assets in relation to critical national infrastructure sectors especially classified information are identified and documented.
Trust	Domestic Hosting and Domains	The Government must enforce critical infrastructure owners to use Domestic Hosting and Domains, such as the use of ccTLD Indonesia to demonstrate data sovereignty within national jurisdiction.	This requirement helps ensure that reasonable effort has been made to protect the whole people of Indonesia and the entire homeland of Indonesia.

2) ANALYSIS AND DISCUSSION

The development of National Hosting and Domains such as a national email service and national hosting would allow Indonesian citizens to keep their data within areas of national jurisdiction. In this way, Indonesian authorities take reasonable efforts to keep the citizen's data out of the reach of foreign companies. These efforts also take positions beyond the domination of the U.S. global infrastructure networks and services. One interesting result is that panellists stated

a preference for the use of Indonesia's national Top Level Domain (.id).

With regard to state self-defence, there are several risk scenarios that need to be addressed. Without a national security risk assessment and determination of national threat levels, information security policy and standards may not adequately cover the requirements of state self-defence. The best approach that the government can take is to manage and mitigate threats and risks against communications surveillance. It seems that managing risks can identify and respond against potential national threats and existing vulnerabilities.

Another important risk factor is a lack of a culture of trust that can lead to a risk of over-control. If combined with other risks such as lack of compliance to security baseline, lack of clarity around escalation procedures, it creates a number of vulnerabilities. Therefore, state self-defence governance requires very detailed and rigid requirements with numerous security controls designed to cover the governance element in relation to state cyber-defence requirements. We summarise risk associated with the requirements in Table 6.

We found that some security controls such as ISO-27001 and NIST SP800-53 fit these requirements, except the Critical Security Controls. One novel requirement was encouraging national domain names usage. Therefore, there is no related security controls placed in relation to this requirement. A summary of appropriate controls is contained in Table 8.

E. LEGAL REMEDIES

We asked panellists to discuss legal remedies. We identified five legal requirements intended to improve the depth of legal remedies for internal and external persons. The majority preference was to include information security agreement, regulation of data protection, data centre localisation, lawful intercept capability and laws, and develop a Bilateral Code of Ethics and Conduct, which will likely map out future protocols over electronic surveillance and intelligence gathering. The requirements focus on contractual service agreements, due diligence obligations to the national legal framework, and lawful interception capabilities.

1) RESULTS

We found the requirements in relation to Legal Remedies as follows:

1) Information Security Agreement (ISA);
2) Regulation of Data Protection (RDP);
3) Data Centre Localisation (DCL);
4) Lawful Interception Capability (LIC);
5) Code of Ethics and Conduct (CEC).

Detailed requirements in Legal Remedies are summarised in Table 7.

TABLE 7. Risk and requirement of legal remedies.

Risk	Requirement	Description	Reasonable Effort
Agreement	Information Security Agreement	The Government must provide evidence that information security agreement between critical infrastructures and related parties are in place to minimise risks of foreign surveillance.	This requirement helps ensure that availability of information security agreement must be in place for any critical national infrastructure sectors such as defence and telecommunications.
Data Protection	Regulation of Data Protection	The Government must provide evidence that a set of data protection requirements has been established for which of data in which contexts can be collected and stored by organisations.	This requirement helps ensure that due diligence against data protection must be in place to protect security and privacy of information. services.
Cross Border Information	Data Centre Localisation	The Government must provide evidence that a set of requirements has been established to place a data centre and disaster recovery centre in the country.	This requirement helps ensure that the obligation to place a data centre, and disaster mitigation centre locally must be in place for the purpose of law enforcement, protection and sovereignty of the state and its citizens.
Lawful Interception	Lawful Interception Capability	The Government must provide evidence that lawful intercept capability laws are in place to enable necessary and proportionate communications surveillance by intelligence and law enforcement agencies.	This requirement helps ensure that an intelligence collecting process is in place. It should include mechanisms for lawfully obtaining raw data, as well as any privacy constraints.
International Cooperation	Code of Ethics and Conduct	The Government must provide evidence that a set of protocol and code of ethics has been established for establishing bilateral cooperation with other countries.	This requirement helps ensure that effort has been made to protect classified information that cannot be disclosed under the law.

2) ANALYSIS AND DISCUSSION

An effective legal and regulatory environment must be in place to encourage good information security practice as well as to establish resilience requirements to support delivery of critical information protection.

Legal remedies, in conjunction with a data localisation requirement, is part of protecting and safeguarding national interests. In addition, the availability of information security agreements between Indonesian organisations and foreign entities must be in place for the organisation in relation to critical national infrastructure sectors such as public services, defence, energy, and telecommunications. We summarise risks associated with the requirements in Table 7.

It seems clear that every state must build their own best capacity to protect national interests against foreign intelligence services as well as to conduct surveillance activities in support of its own interests. However, it is important to bear in mind that such intelligence agencies also have an important role in safeguarding and protecting the state's national interests such as protecting national security, ensuring the economic well being of the state, and preventing serious crime. Therefore, initial efforts have been made by the government to address the current surveillance programmes of the foreign intelligence services, such as data protection regulation, information security agreements, data centre localisation and a Bilateral Code of Ethics and Conduct, which will map out future protocols over electronic communications surveillance.

We identified that only ISO-27001 and NIST SP800-53 cover these requirements and none from Critical Security controls fit these requirements, except control 17 data protection. A summary of related controls is listed in Table 8.

TABLE 8. Mapping requirements for other security controls sets.

ID	Requirement	National Interests				Mapping to		
		NI1	NI2	NI3	NI4	ISO 27001:2013	NIST SP 800-53 Rev.4	CCS CSC
1	Awareness, Training and Education	X		X		A.6.1.1 A.7.2.2	AT-1, AT-2, AT-3 PS-7, SA-9, PM-13	CCS CSC 9
2	Information Security Commitment	X		X		A.5.1.1, A.6.1.1 A.7.2.1	PM-1, PM-2, PM-3	None
3	Non-Disclosure Agreement	X		X		A.13.2.4	PS-6	None
4	Proof of Security Clearance	X		X		A.7.1.1	PS-3, SA-21	None
5	Local Experts Requirement	X		X		None	None	None
6	Trustworthy Systems Certification	X			X	A.14.2.8, A.18.2.1, A.18.2.2, A.18.2.3.	SA-13, CA-2, CM-4	None
7	Registration of Authorised Software	X			X	A.8.1.1, A.8.1.2, A.14.1.1, A.14.1.2, A.14.2.6	CM-8, CM-10, SA-3, PM-5	CCS CSC 2
8	Registration of Authorised Hardware	X			X	A.8.1.1, A.8.1.2, A.14.1.1, A.14.2.9	CM-8, IA-3, SA-4 SI-4, PM-5	CCS CSC 1
9	Incident Response Management	X			X	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6	IR-4, IR-6, IR-8, AU-6	CCS CSC 18
10	Security Continuous Monitoring	X			X	A.12.2.1, A.12.4.1, A.12.6.1, A.14.2.7, A.15.2.1	SI-3, AU-6, AU-13 RA-3, RA-5, SA-9, SA-11,SA-12,CA-8	CCS CSC 4, 5 CCS CSC 14 CCS CSC 16
11	System and Communications Protection	X	X			A.8.2.3, A.13.1.1 A.13.2.1, A.13.2.3 A.14.1.2, A.14.1.3	PE-20, SC-8, SC-7, SC-11, SC-28, CA-3, SC-13	CCS CSC 17
12	National Cryptographic Standards	X	X			A.10.1.1, A.10.1.2 A.14.1.2, A.14.1.3 A.18.1.5	SC-12, SC-13, SC-17	CCS CSC 17
13	Local Applications Platform	X	X			None	SC-27	None
14	National Infrastructure Platform	X	X			None	None	None
15	Control of International Traffic	X	X			None	None	None
16	Agency of Independent Review	X	X		X	A.14.2.8, A.18.2.1 A.18.2.2, A.18.2.3	CA-1, CA-2, CA-7 SA-11	None
17	Risk Management Process	X	X		X	A.12.6.1	PM-9, PM-8, SA-14 RA-3	CCS CSC 4
18	Information Security Baseline	X	X		X	A.14.1.1, A.14.2.5	PL-2, PL-7, PL-8, SA-8	CCS CSC 3, CCS CSC 10, 11
19	Impact of Potential Threat	X	X		X	A.11.1.4, A.12.6.1, A.17.1.1, A.17.2.1	CP-2, PM-9, RA-3	CCS CSC 8
20	Domestic Hosting Domains	X	X		X	None	None	None
21	Information Security Agreement	X	X		X	A.13.2.2, A.15.1.2	SA-4, SA-12, PS-6, SA-9	None
22	Regulation of Data Protection	X	X		X	A.8.2.1, A.18.1.4	SI-12, RA-2	CCS CSC 17
23	Data Centre Localisation	X	X		X	None	None	None
24	Lawful Interception Capability	X	X		X	None	None	None
25	Code of Ethics and Conduct	X	X		X	A.18.1.1	None	None

In summary, the requirements identified by participants for mitigation of foreign surveillance activities were clear. Many of these are common to other scenarios, and have been identified in information security best practice. A mapping to three different cyber security standards is summarised in Table 8.

This study found twenty-five Indonesian requirements for state self-defence to mitigate foreign surveillance activities. The requirements provide a series of significant notions of the national interest. In this case, As stated in the preamble of the 1945 constitution of the Republic of Indonesia, Indonesia's national aspirations aim as follows[3]:

1) To protect the whole people of Indonesia and the entire homeland of Indonesia (NI1).
2) To advance general prosperity (NI2).
3) To develop the nation's intellectual life (NI3).
4) To contribute to the implementation of a world order (NI4).

In addition, the implementation of state cyber defence requirements may result in better means of mitigation of foreign surveillance activities and increased public trust in cyber security and privacy practices. The government acknowledged that concrete steps are needed to meet and implement these main requirements. Encouraging in this regard is the observation that some governmental institutions have already started implementing some requirements as described in the state self-defence framework. It is inevitable that the implementation of improvements will take time and may differ in details between organisations.

The outcome of the state cyber-defence requirements study may be helpful to identify those requirements in national security risk assessment that will potentially influence policy-makers' views on the mitigation of foreign surveillance. The emphases placed on these requirements were prominent to extend that panellists referred to them as 'basic' requirements for state self-defence.

Beyond these requirements, it is difficult to order the remaining factors universally across all four panels with much statistical confidence. The panellists were also asked to rate requirements statements on a sliding scale of 'importance'. In doing so, panellists were allowed to state the same requirements. These results were not useful for ranking purposes, but did help to classify some requirements according to their relative importance. Using this scale, three factors stood out as receiving a high rating from all panels: (1) Security Awareness, (2) Regulation on Lawful Interception, and (3) Strong Leadership.

Given the importance attributed to these requirements, there is certainly justification for further research to determine the means by which governments can ensure those requirements can be implemented effectively in order to mitigate foreign surveillance activities.

VI. CONCLUSION

We have described a variant of the wideband Delphi estimation and traditional Delphi study, adapted to understand policymakers' requirements for state cyber-defence against foreign intelligence surveillance. The variant includes three rounds of the Delphi technique in order to achieve convergence among experts, along with review and approval from policymakers. Testing this method with the Indonesian government, we found that further rounds would have yielded diminishing returns, particularly in terms of panellist participation.

Our Indonesian government, industry and academic expert participants identified mitigation controls in relation to the five-defence in depth elements: people, operations, technology, governance and legal remedies.

The People element is a current weakness in Indonesia. Creating a security mind-set and a culture of cyber security awareness within the organisations are the biggest challenges. If ''people are the weakest link'' and ''security is only as good as its weakest link'' [42], it means the government must better prepare society for information security. This is due to the fact that people may also be the greatest strength when organisations are able to develop a culture of cyber security. Therefore, it is important to promote ethical behaviour and employee vigilance against cyber threats.

[3]These four goals are in accordance with Indonesia's national interests (NI).

Our participants identified operational measures that should be taken to protect critical information, including a formal definition of national critical information infrastructures. It is somewhat surprising that participants did not present a consensus definition, which may be due to the absence of a national cyber security strategy. We suggest that the government should develop standards and incident handling capabilities to deal with the threats discussed.

Security mechanisms are needed to protect critical information infrastructures that may impact state sovereignty, and people's safety, prosperity, and well-being. The location and potential path of classified information must be understood in order to implement technical measures. This allows various technical controls to be implemented to protect critical information in layers.

A lack of strong leadership including governance and coordination exists due to ambiguity concerning shared responsibilities. The government should establish and maintain an information security governance framework to overcome this.

Finally, even though Indonesia has passed a number of laws addressing information security (the Telecommunications Law Number 36 of 1999, the Information and Electronic Transactions Law Number 11 of 2008, and the Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012), Indonesia is particularly weak in legal measures, especially lawful interception capabilities. A considerable effort has been made to create the Bill concerning Lawful Interception, though it has been a controversial addition to the laws because it contains provisions that can harm human rights and privacy in communications. The government can carry out lawful interception to protect and safeguard the state's national interests as well as to prevent crime in accordance with the laws. Therefore, strong regulation is an essential part to protect the country from threats and indeed part of strong defence.

The question remains whether the requirements identified can be implemented effectively to mitigate passive communications surveillance. A controlled assessment in the areas of people, operations, technology, governance, and legal remedies for defence in depth will be required to implement the selected requirements. Responsible stakeholders will need to be identified, and the requirements linked with example control references such as existing regulation, standards, guidelines, and practices.

In future investigations, it might be possible to further develop our variant Delphi approach to investigate to what extent governments can protect national security and privacy in cyberspace, and to examine the fundamental and essential elements of sovereignty in cyberspace.

ACKNOWLEDGMENT

Many thanks to Andrew Martin and Frederick Wamala for their helpful comments on a draft of this paper. The authors would like to thank the anonymous panellists for their participations in this study. The views expressed on this paper are those of the authors and do not reflect the official policy or position of the Government of Indonesia. Any errors, of course, remain our own responsibility.

REFERENCES

[1] *Defense in Depth*, National Security Agency, Fort Meade, MD, USA.
[2] *Information Assurance Technical Framework*, National Security Agency, Fort Meade, MD, USA, 2000.
[3] *Signals Intelligence*, National Security Agency, Fort Meade, MD, USA, 2009.
[4] E. Amoroso, *Cyber Attacks: Protecting National Infrastructure*. Amsterdam, The Netherlands: Elsevier, 2012.
[5] Z. Bauman *et al.*, "After Snowden: Rethinking the impact of surveillance," *Int. Political Sociol.*, vol. 8, no. 2, pp. 121–144, 2014.
[6] B. W. Boehm, *Software Engineering Economics*. London, U.K.: Prentice-Hall, 1981.
[7] I. Brown, "The feasibility of transatlantic privacy-protective standards for surveillance," *Int. J. Law Inf. Technol.*, 2014, pp. 1–18, Sep. 2014.
[8] D. Campbell, "Interception 2000: Development of surveillance technology and risk of abuse of economic information," Director General Res. Eur. Parliament, Luxembourg, Tech. Rep. PE 168.184, Oct. 1999.
[9] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Softw. Eng. Inst., DTIC, Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2007-TR-012, 2007.
[10] B. D. Caulkins, "Proactive self defense in cyberspace," DTIC, U.S. Army War College, PA, USA, Tech. Rep. No. 0704-0188, 2009.
[11] N. C. Dalkey, B. B. Brown, and S. Cochran, *The Delphi Method: An Experimental Study of Group Opinion*, vol. 3. Santa Monica, CA, USA: RAND Corp., 1969.
[12] J. Feigenbaum and J. Koenig, "On the feasibility of a technological response to the surveillance morass," in *Proc. 22nd Int. Workshop Secur. Protocols*, Cambridge, U.K., 2014, pp. 239–252.
[13] *National Cyber Security Strategies in the World*, European Union Agency for Network and Information Security, Brussels, Belgium, 2013.
[14] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, Standard ISO/IEC 27001:2013, 2013.
[15] M. Gidda. (2013). *Edward Snowden and the NSA Files—Timeline*, The Guardian, London, U.K. [Online]. Available: http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
[16] T. D. Gill and P. A. Ducheine, "Anticipatory self-defense in the cyber context," *Int. Law Studies (U.S. Naval War College)*, vol. 89, pp. 438–471, 2013.
[17] M. J. Glennon, "Fog of law: Self-defense, inherence, and incoherence in article 51 of the United Nations charter," *Harvard J. Law Public Policy*, vol. 25, pp. 539–558, 2001.
[18] T. Gordon and A. Pease, "RT Delphi: An efficient, 'round-less' almost real time Delphi method," *Technol. Forecasting Social Change*, vol. 73, no. 4, pp. 321–333, May 2006.
[19] D. E. Graham, "Cyber threats and the law of war," *J. Nat. Secur. Law Policy*, vol. 4, pp. 87–102, 2010.
[20] A. N. Guiora, "Self-defense—From the wild west to 9/11: Who, what, when," *Cornell Int. Law J.*, vol. 41, no. 3, p. 631, Aug. 2008.
[21] J. F. Hill, "The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and business leaders," in *Proc. Hague Inst. Global Justice, Conf. Future Cyber Governance*, 2014, vol. 2, no. 3, pp. 1–41.
[22] S. Hoermann, M. Aust, M. Schermann, and H. Krcmar, "Comparing risks in individual software development and standard software implementation projects: A Delphi study," in *Proc. 45th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2012, pp. 4884–4893.
[23] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House, Washington, DC, USA, 2011.
[24] J. P. Kesan and C. M. Hayes, "Mitigative counterstriking: Self-defense and deterrence in cyberspace," *Harvard J. Law Technol.*, vol. 25, no. 2, p. 429, 2011.
[25] J. Landeta, "Current validity of the Delphi method in social sciences," *Technol. Forecasting Soc. Change*, vol. 73, no. 5, pp. 467–482, 2006.
[26] *Defence in Depth*, Trusted Information Sharing Network, ACT, Australia, 2008.

[27] *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2013.
[28] C. Okoli and S. D. Pawlowski, "The Delphi method as a research tool: An example, design considerations and applications," *Inf. Manage.*, vol. 42, no. 1, pp. 15–29, 2004.
[29] *Critical Security Controls for Effective Cyber Defense*, Council on CyberSecurity, Arlington, VA, USA, 2009.
[30] A. M. Rutkowski, W. A. Foster, and S. E. Goodman, "Multilateral cyber solutions: Contemporary realities," in *Public Interest Rep.*, vol. 65, no. 1, pp. 12–18, 2012.
[31] R. Schmidt, K. Lyytinen, M. Keil, and P. Cule, "Identifying software project risks: An international Delphi study," *J. Manage. Inf. Syst.*, vol. 17, no. 4, pp. 5–36, 2001.
[32] A. Stellman and J. Greene, *Applied Software Project Management*. Sebastopol, CA, USA: O'Reilly Media, Inc., 2005.
[33] M. G. Stochel, "Reliability and accuracy of the estimation process—Wideband Delphi vs. Wisdom of crowds," in *Proc. 35th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2011, pp. 350–359.
[34] N. Taylor, "To find the needle do you need the whole haystack? Global surveillance and principled regulation," *Int. J. Human Rights*, vol. 18, no. 1, pp. 45–67, 2014.
[35] G. H. Todd, "Armed attack in cyberspace. Deterring asymmetric warfare with an asymmetric definition," *AFL Rev.*, vol. 64, p. 65, Jun. 2009.
[36] *Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies*, International Telecommunications Union, document Rec. RESOLUTION 130, 2010.
[37] F. Wamala, *ITU National Cybersecurity Strategy Guide*, International Telecommunication Union, Sep. 2011.
[38] L. Williams, A. Meneely, and G. Shipley, "Protection poker: The new software security 'game,'" *IEEE Security Privacy*, vol. 8, no. 3, pp. 14–20, May/Jun. 2010.
[39] E. Ziglio, "The Delphi method and its contribution to decision-making," in *Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health*. London, U.K.: Jessica Kingsley, 1996, pp. 3–33.
[40] Statistics Indonesia, *Statistical Yearbook of Indonesia 2014*. Jakarta, Indonesia: Central Agency on Statistics, 2014.
[41] Indonesia Internet Service Provider Association. (2013). *Indonesia Internet Users*. [Online]. Available: http://www.apjii.or.id/v2/read/page/halaman-data/9/statistik.html
[42] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*. New York, NY, USA: Wiley, 2000.

YUDHISTIRA NUGRAHA (M'14) received the B.E. degree in telecommunications engineering from Telkom University, Bandung, Indonesia, in 2003, and the master's degree (Distinction) in information and communication technology advanced from the University of Wollongong, Wollongong, NSW, Australia, in 2009. He is currently pursuing the D.Phil. degree (Oxford's PhD) in cyber security with the Department of Computer Science, Centre for Doctoral Training in Cyber Security, University of Oxford, Oxford, U.K. He has been an Engineer, a Researcher, and an Assessor in the field of information technology and telecommunications. He is a Certified ISMS Auditor and Certified Ethical Hacker. He has served as the Head of Information Security Risk Management with the Directorate of Information Security, Ministry of Communications and Information Technology, Jakarta, Indonesia. His research interests are in the areas of information security and privacy, requirements engineering, and cyber governance. He is a member of the Association for Computing Machinery, the Professional Evaluation and Certification Board, and the Institute of Information Security Professionals.

IAN BROWN received the Ph.D. degree in computer science from University College London, London, U.K. He is currently an Associate Director of the Cyber Security Centre and a Professor of Information Security and Privacy with the Oxford Internet Institute, Oxford University, Oxford, U.K. His research is focused on surveillance, privacy-enhancing technologies, and Internet regulation. He is an ACM Distinguished Scientist and BCS Chartered Fellow, and a member of the Information Commissioner's Technology Reference Panel. He has acted as an expert witness for the English High Court, the U.K. Investigatory Powers Tribunal, and the European Court of Human Rights, and given evidence to the U.K., German, and European parliaments. Since 2014, he has been a Knowledge Exchange Fellow with the Commonwealth Cybercrime Initiative and the U.K. National Crime Agency.

ASHWIN SASONGKO SASTROSUBROTO received the B.E. degree in electrical engineering from the Bandung Institute of Technology, Bandung, Indonesia, and the M.Sc. and Ph.D. degrees in power electronics from Aston University, Birmingham, U.K. He has served as the Director General of Informatics Application with the Ministry of Communications and Information Technology (MCIT). He served various positions with the government as the Secretary General of the MCIT, the Secretary to the Ministry of Research and Technology, the Deputy Minister with the State Ministry for Communication and Information, and the Vice Chairman of the Agency of Application and Assessment of Technology. He is currently a Senior Researcher with the Indonesian Institute of Sciences and the Chairman of the Study Centre of Public Policy and ICT Business with Telkom University, Bandung. He is also a member of the National ICT Council. His current interests are in electronic systems, ICT governance, and cyber security policy.