POSITION PAPER

Case for a Trustless Computing Certification Body

Can a new certification body deliver radically unprecedented IT security for all, while at once ensuring legitimate lawful access?

Version 1.0 *(April 30th 2018)*

Abstract: *In this position paper, we argue that a new cybersecurity certification body can, and should, be created which will be able to reliably and sustainably certify end-to-end IT services with levels of integrity and confidentiality that radically exceed current state-of-the-art, civilian and military, while at once solidly enabling only legitimate and constitutional lawful access. Both can be achieved through uniquely uncompromising "zero trust" security-by-design paradigms down to each critical lifecycle component, including the certification governance itself.*

Authors: Rufo Guerreschi and Udit Dhawan. (See below for profiles and contributors)

Executive Summary 1-pager

Recent revelations and reported security breaches have highlighted the fact that even the most stringent current IT security certifications are severely inadequate in their ability to: (a) afford citizens and organizations access to IT services and devices that can meaningfully protect their **fundamental civil rights,** (b) enable governments to reliably enforce their own regulations aimed at the defense of democratic sovereignty, security agencies' capabilities and oversight, criminal prosecution, critical infrastructure, and integrity and efficacy of **targeted cyber-investigations**, and (c) enable an adequate security baseline for the regulation or certification of the most critical deterministic sub-systems of advanced **security-critical AI systems**, given their huge societal implications.

Goals (a) and (b) have increasingly revealed themselves as interlinked, since the failure of current IT security certifications to provide (a) has been in fact overwhelmingly due to at-all-costs efforts by powerful nations to retain cyber-investigation capabilities through remote and local "lawful hacking". This has in turn prevented such endpoint cyber-investigation capabilities to achieve the required levels of integrity of evidence so acquired to stand the scrutiny of constitutional courts, and their own required resistance from external and internal abuse to foster the level of international intelligence exchange needed to best prosecute grave international crimes.

In this position paper, we argue that **a new cybersecurity certification body,** the Trustless Computing Certification Body ("**Certification Body**" or "**TCCB"**), could and should be created. It should be suitable to confidently certify end-to-end IT services that are able to sustain levels of integrity and confidentiality radically exceeding current state-of-the-art in their resistance against state-grade remote or local hacking. It should also be suitable for the responsible exercise of citizens' privacy, assembly, communication and political rights, except for the most sensitive political and institutional voting.

Key paradigms will center on uniquely ultra-high levels of **transparency, accountability and oversight** of all critically-involved technologies, procedures and people. These include **ultra-high ethical, expert and public security-review in relation to complexity**", advanced citizen-witness and citizen-jury-like oversight processes, online and in-person multi-jurisdictional secret-sharing techniques. Economic feasibility is granted by radical minimization of features and performance, effective compartmentation, and critical technical stacks that are time-proven and subject to open IP regimes.

Compliant providers - in order to prevent crimes, stave off its outlawing and cater to user need for safer key recovery - will be mandated to voluntarily (i.e. in excess of legal obligations) offer to national security agencies evaluation of their lawful access requests for adherence to law and international human rights, through an **offline key or data escrow/recovery process**. By applying the same safeguards used to ensure ultra-high security, and more, the inevitable added risk will be radically mitigated, resulting in compliant IT services that **overall** reduce the risk of abuse of end-users by anyone to levels that are **radically (or at least substantially) lower than any of the other alternative secure IT systems - available today or knowingly in development - which do or do not offer such voluntary processing**.

Contents

1 Stating the Case for a Trustless Computing Certification Body

Five years have passed since Snowden revelations. As opposed to what most media, security agencies and secure IT providers report, while unbreakable end-to-end encryption is everywhere, nearly every IT system is scalably broken, at birth, and mostly by design.

Recent Intel, AMD[1] and Ledger[2] hacks reveal how critical vulnerabilities and state-inserted or *state-allowed* backdoors run deep, **down to CPUs and chip fabrication**. Meanwhile Shadow Brokers and CIA Vault 7[3] revelations, and the hacks of Hacking Team[4] and Greyshift[5], have further shown how state-grade critical vulnerabilities are **ever more widely-available to even mid-level criminals**, in scalable ways. For every critical bug publicized by a student in the most secure mainstream phone [6], how many others are out there illegally exploited by criminals and states?

While most mainstream civil rights activists celebrate their having prevented **state-mandated backdoors** in all IT systems - and rejoice on highly insecure "end-to-end" secure systems, from iPhone, to Signal to Tor - no device exists that plausibly does not have **state-inserted or *state-allowed* backdoors**, in the form of critical vulnerabilities that are let be via collusion, purchase, subversive insertion, discovery and ultimately stockpiled.

Even worse, their inability to safely stockpile and the huge direct and indirect **growth of the vulnerabilities market**, radically increases the vulnerability of citizens, businesses, active citizens, and politicians.

1.1 The dire need and demand for radically more secure IT and AIs

Although, private cybersecurity spending has grown 30 times in the last 10 years to $120 billion[7] in 2017, the cost of **cybercrime** will skyrocket to a forecasted $6 trillions[8] per year in 2021. Not to mention the cost to our ordinary and active citizens rights democratic institutions, which seem held at ransom from state and non-state groups, each accusing the other.

A recent PwC survey highlighted how "*investors see cyberthreat as the main obstacle to enterprise growth*". The CEO of IBM stated that "*Cybersecurity has become the greatest threat to any company in the World*".

Recently, the **German Minister of Defense identified cyberattacks as the "*single greatest threat to global stability***". This is not surprising given the increasing vulnerability, complexity and lack of adequate standards for critical civilian and military systems, which makes them not only overly vulnerable but also their hacking inherently very difficult to attribute. The inadequate standards, obscurity, hyper-complexity, and *forensic-unfriendliness* of even the most critical systems and processes, in fact, renders **state-grade cyber-incidents very difficult to attribute** in an internationally recognized way, as International Atomic Energy Agency and the International Criminal Court have enabled, at least partly, for nuclear and war crime incidents.

While it is increasingly clear that **those with superiority in Artificial Intelligence will rule the world** - as stated by Vladimir Putin[9] - the surprising hacking prowess demonstrated by certain nations and groups, and the astonishing vulnerability of the most critical systems and processes of the most powerful nation in the world, leads one to believe that **informal control of advanced AIs through sustained malicious hacking capabilities** may turn out to be even more decisive than their formal control through ownership and design.

The **world is rapidly turning into a Hacker Republic.** On one hand, most political and economic power accrues to those with sustained **informational and *malicious* hacking superiority** in critical communications and AI systems, resulting in a huge asymmetry of power between them and all others, creating two sets of citizens. On the other hand, ***ethical* hackers and whistleblowers** serve crucial public service to reign in such power by informing citizens and legislators, through revelations about critical vulnerabilities, unconstitutional state surveillance programs, and unearthing mass-scale crimes and frauds of the rich and powerful.

1.2 Myths about the most secure commercial IT systems, and their resistance to scalable hacking by a large number of attackers

Over the last few decades, the IT security community has made significant breakthroughs to enhance the security (in terms of confidentiality and integrity) and trustworthiness of IT services and devices. These include advances in **end-to-end encryption**, forward secrecy, **blockchains**, **anonymization networks**, and **formal verification** in hardware and software designs. However, nearly all systems are still vulnerable to the kinds of subversions that these technologies were meant to prevent, as is evident from recent revelations and reported security breaches, and significant increases in cybersecurity spendings and cost of cyber-thefts over the last few years alone.

In fact, their regular use involves or requires numerous **uninspectable and/or insufficiently-inspected critical components and processes** throughout the life-cycle of the endpoint devices. Worse, those techs often turn out to be ways to self-flag oneself[10] for special scrutiny by overreaching security agencies or criminals. In 2013, Edward Snowden said, "*Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it".*

Many privacy activists and experts have arguably over-relied on a few statements on leaked NSA documents and self-serving declarations of security agencies to quickly conclude that advanced attackers are highly constrained in their scalable use of most or all targeted exploitation techniques to avoid burning them.

But careful analysis of the (2009!) capabilities of **NSA Turbine**, **NSA FoxAcid**[11], tools or their private equivalents like **Hacking Team RCS**[4] shows how it is highly probable that advanced endpoint exploitation techniques and tools allow them to **scale to hundreds of thousands** and prevent such "burning" risk by using exploits that are beyond the ability of the target to discover, and other techniques.

Even if such scaling capabilities were lower than reported, it can be argued that the value of spying the world's 10,000 most "valuable" current and prospective activists, politicians, billionaires and their direct acquaintances, is much higher than for the other 7 billions.

In 2014, one of those leading experts and activists, **Jacob Appelbaum**, who had an unfiltered view of part of Snowden documents, clearly stated[12] : "*It does seem to indicate to me that cryptography does stop them ... I have seen that the Tor browser stops them from doing passive monitoring, and they have to switch to targeted. And that's good. We want them to go from bulk, or mass, surveillance* *to targeted stuff. Now, the targeted stuff, because it is automated, is not different in scale but just different in methodology, .. actually. And usually they work together".*

So therefore, civilian end-to-end encryption and anonymizations solutions like Signal, Telegram, PGP, Tor, or the most secure devices or open source device setups - such as those by Samsung, Apple, Thales, Silent Circle, Sirin Labs, Athos, General Dynamics, Boeing, TailsOS, Qubes OS, etc. - do not provide nearly sufficient arguments, proof or indication that they are plausibly beyond being hacked or circumvented by a large number of attackers.

1.3 Myths about the most critical governmental IT systems

Michael Sieber, former (2012-2016) Head of Information Superiority of the European Defence Agency. stated at the 1st Free and Safe in Cyberspace conference in 2015: "*Among EU member states, it's hilarious: they claim digital sovereignty but they rely mostly on Chinese hardware, on US American software, and they need a famous Russian to reveal the vulnerabilities*"[13].

Even devices and systems certified by **highest EU and NATO certifications** with strictly limited commercial availability, are also plausibly vulnerable; though to a smaller number of threat actors because, they have fewer and deeper uninspectable and/or insufficiently-inspected critical components and processes. In fact, even **certifications for such system utilise are structurally inadequate** in their depth and comprehensiveness of technical and socio-technical stacks; largely self-referential; reliant on state and private certification labs with semi-captive relationships with providers and hosting nations; and often biased by the addition of "national crypto standards".

Their inadequacy and vulnerability is nearly always not advertised publicly, and successful hacks of such systems, even when detected internally, nearly always become state secret. An additional evidence is the fact that Italy and Austrian bodies deputed to set such standards, have been governance partners of EU R&D proposals to realize the dual-use Certification Body since 2016 being presented here[14].

The only exception are very limited use cases of well-funded and very expert and prepared individuals and entities, and mostly for limited use cases. These exceptions are exceedingly small in number, as shown by how even the most rich and most powerful were fooled for decades by the likes of the Swiss **Crypto AG**[15], with its tapped cryptophones, or **Promis Inslaw**[16], with its *lawful hacking* platforms, and revelations of NSA tapping of **president of Brazil and chancellor of Germany**, and that even the leaders of the **US Democratic Party**[17] did not have ways to communicate securely and effectively.

The only reliable measure of the effectiveness of an high trustworthiness IT security provider, private and public, relies on its "closeness" to major stockpilers of critical vulnerabilities - i.e. mostly a few large powerful states like US, Israel, China and Russia - creating pervasive intelligence **network effects**[18], gravely undermining society sovereignty, freedoms and competitiveness.

1.4 Why most believe current systems and certification to be much more secure than they are?

A mix of powerful governments self-serving "partial" information to induce criminals and even other nations' official to misuse systems they believe to be non interceptable - and the untruthful marketing and baseless claims of proprietary and open source *secure* IT solutions - has brought most of the public and experts to believe that the best available systems - commercial and highest-grade certified governmental devices alike - offer much more protection than they actually do.

The ethical hacking, free/open source and digital civil rights activist communities public statements on the security of the best open/source secure communication solution have been wildly overstating their security levels, because of: strong dynamics of groupthink, peer-pressure, as well as conflict of interest, and extensive economics funding from US government and large US IT giants.

Furthermore, these activist communities are dominated by very minoritation libertarian or anarchic political views and cyber-libertarian ideologies, which have lead them to believe that digital civil freedoms can be self-enforced through more and better open source software and open hardware, without the need for any sort of formal democratic control and oversight organizations.

1.5 The inescapable *de-facto* reliance of any IT service security on "trusted third-parties"

The ethical hacker and digital civil rights activist communities are dominated by the view of die hard cyber-libertarian fans of **end-to-end encryption** or **blockchains** - that "decentralized" cryptographic protocols, open source, end-to-end encryptions and other techniques *de facto* enable individuals and groups to do away with the need to critically rely on **any** "trusted third" party -- to somehow individually self-deliver meaningiful security and freedoms.

The obscure and unaccountable ways in which such decentralized and end-to-end crypto systems providers manage their **firmware updates** makes them scalably vulnerable to be exploited by the provider itself, rogue employees, criminals or nations; and in a way it is very difficult to prove what was done in error and what by accident. Prof. Villasenor highlighted[19] that the way Apple currently manages firmware upgrades amounts to a backdoor.

A recent test by Security Research Labs on 1200 Android phones from a dozen makers found that all but one[20] contained all the security patches as advertised. Millions of Macs did not report the failure to update of their firmare[21]. The famous FBI/Apple apparent spat over the San Bernardino case brought many to view the obscure processes by which firmware upgrades are managed as a backdoor

A 2014 blog post *Cyber-libertarianism vs. Rousseau's Social Contract in Cyberspace[22]* argues how that is impossible because of **the inherent complexity of IT supply chains and life-cycles creates one or more organizations and sociotechnical processes that have a role of "trusted third-party".**

The famous cryptographer Bruce Schneier - in this Feb 2017 video[23], at minute 22.40 - describes how he recently changed his mind realizing how highly-trustworthy "trusted third-party" organizations and socio-technical systems are an inevitable necessity to achieve meaningful security for IT and blockchains, given the many socio-technical and governance processes that are critically involved in the lifecycle of such decentralized systems, and their real-life usage scenarios, that greatly affect their resulting security levels.

It follows that it becomes crucial that the **main challenge is therefore to make such "trusted third-parties" as *trustless* and trustworthy as possible**. They should be therefore designed, organizationally and socio-technically, to achieve extreme levels of trustworthiness by ensuring extreme levels of resiliency, comprehensiveness, citizen-accountability and competency, including through the extensive use of **citizen-witness** and **citizen-jury-like** processes.

1.6 Introducing the Trustless Computing Certification Body

Our proposed Certification Body is called "trustless computing" to exemplify how only a complete distrustful and untrusting posture - as practiced for many decades in state-of-the-art voting booth processes and nuclear weapons facility management processes - can deliver the trustworthiness to today's most critical IT systems demand.

1.6.1 Socio-technical breakthroughs

In order to achieve such ambitious security levels, a TC-compliant IT service will be certified and overseen by the Certification Body to ensure that all *critically-involved* technologies and lifecycle processes are subject to extreme levels of **transparency**, **accountability**, **oversight** and **levels of ethical security-review in relation to complexity**.

They would need to be on par or exceed those **successfully** applied to date for the safeguarding of **critical nuclear systems**, best-of-breed **paper-based election processes** and commercial aviation certifications, making extensive use of both online and offline **citizen-witness** and **citizen-jury-like** processes - for hosting room access and for chip fabrication oversight - that are directly accountable and managed by such Certification Body.

1.6.2 Trustless Computing Paradigms - Summary Version

1. *undergoes continuous certification by* an extremely **technically-proficient, comprehensive and citizen-accountable** independent standard-setting and certification body.
2. *assumes* that extremely-skilled attackers are willing to devote even **tens of millions of euros** to compromise its supply chain or lifecycle, through legal and illegal subversion of all kinds, including economic pressures; and advanced algorithmic, brute force and AI-assisted hacking.
3. *provides* extremely user-accountable and technically-proficient **oversight** of all hardware, software and organizational processes that *critically* involved in the entire lifecycle (i.e. including the supply chain). By "critical" we refer to hardware, software or procedures which cannot protect to a very high degree against confidentiality and integrity failures, or abuses, by using by implementing state-of-the-art time-proven OS, SoC and/or CPU level isolation/compartmentation techniques.
4. *provides* extreme levels of intensity, proficiency, ethical **security-review relative to system complexity** for all *critical* components;
5. *includes* only *critical* components that are publicly inspectable in their source designs, and strongly minimizes the use of non-Free/Open-source software and firmware, especially in critical components.
6. *includes* only highly-redundant and decentralized hardware and/or software **cryptosystems** whose protocols, algorithms and implementations are open, long-standing, extensively-verified and endorsed, and with substantial and "scalable" post-quantum resistance levels.
7. *includes* only innovations with **clear and low long-term royalty terms,** from patent and licensing, to prevent undue intellectual property right holders' pressures, lock-ins and vetoes; and sustainably ensure low-cost for affordability by average citizens;

8. *will* provide an **in-person offline key or data recovery function**, to benefit end-users, in case of loss of death or loss passcodes, and to enable a voluntary (i.e. in addition to current law requirements) compliance to legitimate lawful access requests. This function will rely on setups and management process of multiple hosting rooms in multiple jurisdictions that implement unprecedented safeguards. In addition to state-of-the-art security, these will utilize only TC-compliant endpoints and door locking mechanism. Access to such rooms for any reason, always requires the express approval of an attorney and **5 trained citizen-jurors**, that are managed and accountable to the Certification Body - that will assess the compliance of the requests to national law, constitution and EU Charter of Human Rights. Any kind of remote access is physically disabled.

See Trustless Computing Paradigms Full Version, below in section 2.1.

1.6.3 Governance: the all-important factor

By far the most crucial factor affecting the **sustenance and steady increase** of such levels of trustworthiness, and their affordability for all citizens, rests on the ability to **set in place and jump-start initial statutory provisions, bylaws, deliberative cyber-social systems -** since the very initial phase of the Certification Body - so as to maximize on the long-term (decades or more) ultra-high levels of altruistic intentions, technical proficiency and citizen-accountability.

Such Certification Body should therefore be **primarily non-governmental, international** and designed in its statute, constituent process and socio-technical setups in order to sustainably exert a **governance with ultra-high levels of transparency, ethical altruism, technical proficiency, and citizen accountability**; directly, through democratic legislative bodies, and indirectly through direct participation of an informed random-sampled set of citizens. All boards and advisory committees will strive to achieve gender-balanced and some level of worldwide representation.

Therefore the governance of its General Assembly will be so divided:

- 20% by *Ethical & Scientific Advisory Board*, initially composed of the current Trustless Computing Association scientific and ethical advisory board.
- 15% by *Security or Defense agencies of 2 or more democratic nations* (will be offered initially to current TCA governance partners: state secret standard bodies of Italy and Austria. Than Germany. Then others ...)
- 15% by *Data Protection Agencies of 2 or more democratic nations* (will be offered initially to current TCA governance partners: DPA of German State of Schleswig; and then to EDPS, and the DPAs of Italy, German, Austria)
- 15% by *Informed Random-Sampled Citizens*. Made up of 10 random-sampled citizens selected and self-managed according to the *Deliberative Polling*™ method, whereby random-sampled citizens are given an opportunity to self-educate about a matter and then deliberate. They will rotate every 3 months in alternative batches of 5.
- 15% by a *Board of Directors of the Association*. Elected by the Assembly every 12 months.
- 20% by *Active Users of TC-compliant Client Services*. The unique security and authentication levels of TC-compliant devices will in fact enable a safe-enough remote democratic direct participation.

A mandatory TCCB re-constituent assembly every three years - with very clear "re-constituent assembly" election rules - will help remove and counterbalance the inevitable biases and distortions that will inevitably encroach the quality of the governance after years of mounting pressures by very powerful special interests.

1.7 Why nearly all users of ultra-secure IT systems crucially require a data/key recovery service

Even though TC-compliant IT service architectures - in order to comply to the above Paradigms - would be at the core peer-to-peer, end-to-end and decentralized - any compliant IT service will necessarily require the extreme safeguarding of two or more **hosting rooms** - in two or more diverse privacy-preserving jurisdictions - in order to prevent integrity, confidentiality and deletion abuses of sensitive data, logs and systems, such as firmware updates and other critical data, keys, and source code, confidential end-user data, and also, **end-user data/key recovery** information.

The latter is an absolutely necessary utility to all end-users of such ultra-secure IT systems, who would increasingly store their most valuable and sensitive data and digital assets on such devices, and would require **ways to recover access to their data in case their password/key is lost, forgotten or stolen.** Moreover, these utilities will need to be much more efficient and secure than current state of the art.

As per enterprises, banks and governmental institutions, these nearly always firmly require such function to ensure business continuity, for compliance and to enable internal investigations (within legal constraints).

As per consumers, many believe that such key/data recover function would not be desired or necessary, but the weakness and downsides[24] of current state-of-the-art solutions, such as cryptocurrency HW wallet "recovery seed" keys" (whose possession may easily enable to steal tens of millions of dollars in cryptocurrency) - which currently revolves around entrusting fragments of the key to multiple relatives, writing it in a will held by an attorney, *multi-signatures* and/or storing it in a bank safe - show how a "trusted third-party" international organization can easily be devised as a substantially or radically more secure and flexible alternative to these, to be used in conjunction with a will, held by an attorney which indicates the deceased post-mortem intentions for each specific piece of information. In fact, allowing users to manage their "recovery seed" keys in other ways would also compromise all of the user's interlocutors as well.

1.8 How do we prevent such IT to be abused for grave crimes or to be outlawed?

Should such systems be made available in the civilian or governmental markets if there was not a way for security agencies to execute on a lawful access authorization approved by a civilian judge? We believe they should not.

Many activists and ethical experts disagree, as they either (1) do not believe such grave levels of threat exist, or refer to the (2) lack of public evidence that the "gone dark" problem has facilitated grave crimes.

On first issue, history shows that wealthy criminals, crooked politicians, rogue security agencies, terrorists groups would undoubtedly **try to abuse such TC-compliant IT services to facilitate the planning and coordination of grave crimes**, and impede the successful execution of lawful access requests even when duly authorized by a civilian judge. Threats are rising from extremists of all sorts.

A recent Pew survey[25] revealed that over 65M people out of 700M in muslim-majority countries view ISIS favorably. Reports show ultra-nationalist threats are rising in EU, including in Germany[26]. Evidence increases of extensive abuse of power, corruption and subversion by top politicians, heads of state, and even judiciary in some democratic nations such as in the USA [27], Brazil [28], Israel [29]. While illegal or immoral tax practices are revealed by power elites all over the world as revealed by Luxleaks and Panama Papers.

On the second issue, it is not relevant to our argument and proposal. Overwhelmingly, **the "gone dark" or "going dark" cried by security agencies are not true, but useful to them in many ways**: to have more mid-level criminal wildly overestimating existing secure IT, to push legislators to preserve existing lawful access means and acquire new ones (that would produce less contestable evidence) and, possibly, to keep "political adversaries" on an ineffective and defensive posture.

So there is no "gone dark", nor any "going dark" of security agencies but - if we believe that meaningfully-secure IT can actually be built and provisioned - than there is **by definition** a problem of **"could be going dark"**.

All this brings us to a crucial preliminary intuition.

As we argue further, the very same extreme technical, socio-technical and governance safeguards that are needed to certify meaningfully-secure IT can enable such (non-governmental) Certification Body to mandate TC-compliant providers to (voluntarily: in excess of legal obligations) offer to security agencies to process lawful access requests - for legitimacy and adherence to constitution and international human rights Charters - through a **key or data escrow/recovery solution** - while overall reducing the risk of abuse of the users (by states or criminals) to levels that are **radically, or at least substantially, lower than any of of the other alternative secure IT systems -** that are today available, civilian or military - which do or do not offer such voluntary lawful access request processing.

However, most of those same activists and ethical experts believe such voluntary access is not needed to prevent grave crimes. They also believe it is not technically feasible. Many of the top UK/US activist experts have stated and analysed in very detailed papers that it is impossible to so ***"without adding unacceptable additional risk of privacy and security abuse to users and citizens".*** The largest majority of activist IT security professionals, cryptographers and civil rights activists have taken note of this wide consensus and joined to very quickly dismiss a "*lipstick on a pig*" any proposal to solve the dramatic cyber-insecurity of societal most critical IT systems that would include lawful access.

1.9 So is this new certification body a hidden way to push backdoored IT services and devices?

On the contrary, we make a case in this paper that these certifications will spur the wide market availability of the **World's first IT systems and devices that can plausibly be expected to be without backdoors**, state-allowed or state-inserted, for the first time since algorithmically unbreakable encryption was made wide available in the 90's.

Though **perfect security will never exist -** by uniquely implementing extreme transparency, oversight, accountability, and ethical and expert security review in relation to complexity - such certifications will spur the creation of the first IT systems and device that **removes any need or**

assumption upfront unverified trust on anything or anyone along the entire supply chain and lifecycle**.**

In fact, given the extremely high plausible deniability of advanced hacks, it is nearly **impossible to ascertain which critical vulnerabilities are errors due to hyper-complexity or incompetency, or instead are *state-allowed* backdoors** - i. e. critic vulnerabilities that are "let be" through collusion with a provider staff, purchased, licensed; and ultimate stockpiled by nations, and often unsafely (!).

By nature of such tools and techniques - highly impervious to accountability and attribution when skillfully deployed - such **backdoors are wildly abused and abusable** by nations agents and criminals without due legal process. We should therefore assume that all or nearly all devices and services available today are backdoored and hackable by a large number of actors.

Bruce Schneier said in 2014 after reading the raw version of Snowden revelations: "*I assume that all big companies are now in cahoots with the NSA, cannot be trusted, are lying to us constantly*," he said. "*You cannot trust any company that makes any claims of the security of their products. Not one cloud provider, not one software provider, not one hardware manufacturer.* "[30]

As opposed to **all or nearly all other systems, exploitable by nations and criminals without a proper judicial authorization**, such systems will only be offered in privacy-respecting EU nations and deploy radically extreme and transparent technical and organizational safeguards - involving even citizen juries in multiple democratic jurisdictions, accountable to such Certification Body, an highly ethical, international, trustworthy non-profit "trusted third party" - to vet and manage the legitimacy and constitutionality of lawful access requests.

1.10 Why state-mandated technical backdoors or key escrow for all IT are very bad ideas

Since the 1990s, in the legitimate pursuit of extending the same lawful access historically available to all other means of communications to all IP Systems, many national legislative proposals have aimed at mandating key or data escrow solutions or mandated technical systems (like the infamous *Clipper Chip*) inside all IT that enable covert remote access by security agencies into all IT systems sold or introduced in the country.

These proposals, if enacted in laws or treaties, would have a decisive negative impact on both citizens' privacy and for public safety, for the following main reasons:

- The most advanced public security agencies have had, and likely will continue to have, the continuous **capability to break into nearly all endpoints, at nearly all times**, for targeted surveillance; they have in fact needed to resort to such comprehensive capability precisely from the 1990s when unbreakable encryption became popularly available.
- Given the **enormous complexity and diversity of IT systems** and providers, it would be both highly expensive and practically impossible to verify and certify implementations that are sufficiently trustworthy.
- Legislative and public security branches of **government have proven deeply and repeatedly their lack of competency** in architecting technical standards and oversight processes to reasonably limit their abuse.
- **Criminals could still surreptitiously fabricate, modify or import** - or use while abroad - IT systems without such built-in access, and could still pre-encrypt messages externally to the

device or use other means, such as steganography, to communicate covertly over such IT systems.

1.11 How TCCB key/data escrow process differs from other proposals

Two excellent and foundational reports have been written about the feasibility of key or data escrow solutions for lawful access "*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*" [31] and and its subsequent "*Keys Under Doormats*"[32], written by some of the world's top IT security experts. Their analysis is overwhelmingly correct, but it was at times overbroad, possibly intentionally. The scope of their analysis - while often implying a blanket infeasibility of the root concept - left out certain possibilities, such as: additional safeguards, ways to minimize complexity and, especially, the possibility that it could be applied to only for high-grade secure systems that are or could be plausibly beyond targeted state hacking.

Our proposal falls largely out of the scope of such report because it is:

1. **Not regulated, designed, standardized or certified by the state**. Such functions would be managed by a *trusted third-party,* in the form of an extremely technically-proficient and citizen-accountable international standard setting and Certification Body, and by temporary organizational entities made of groups of randomly sampled citizen-jurors and citizen-witnesses, tightly regulated by such body;
2. **Not mandated by the state**. Instead, it is a voluntary practice, i.e. in addition of current legal requirements - by certified ultra-high trustworthiness IT providers, certified by an international Certification Body, and only in selected jurisdictions where laws and practice allow for the provider, or others they delegate, to safely exercise discretion on the basis of constitutionality of the lawful access request;
3. **Not universal for all IT systems but just for ultra-secure ones**. It is reserved only to ultra-high trustworthiness IT services, namely those compliant to the Certification Body, which can truly be expected to be beyond the targeted or large-scale exploitation capability of a large number or all democratic nation states' cyber-investigation agencies.

1.12 Jurisdictional issues, and future roadmap

The Certification Body will initially be deployed to certify IT services in only a few pioneering EU member states, where overbroad (and likely unconstitutional) executive branch powers are *not* in place in law and practice as in the USA; or limitedly so. Nevertheless, it could be soon be extended to certify services offered in such "executive power" nations. In fact, it would still delivering substantial value-added and market adoption, because it would still provide a much increased protection from abuse from threat actors other than an abusive state.

Such "executive power" nations may also decide, at some point, to prescribe that no other means of lawful access can be used - by any public law enforcement and intelligence agency - except those provided by such trusted-third party escrow body; which in turn could further drive their adoption. Such hopes may be warranted by the recent calling by FBI Director Wray of Symphony data escrow model as a best-practice[33] and inspiration.

Our roadmap foresees its adoption as a *certification schema* by the upcoming EU Commission led *European Cybersecurity Certification Framework*. In fact, EU is well positioned to drive global standards on certifications for high-security IT and lawful access - in a similar way as it has done GDPR has done for cloud privacy - as suggested at minute 37.00 of this video[34] by the famous cryptographer Bruce Schneier.

In a later phase, the Certification Body will be extended to certify radically increased levels of trustworthiness for the most critical *root-of-trust* (deterministic) sub-systems of security-critical AI systems.

More details on our proposal for the Trustless Computing Certification Body can be found on our Trustless Computing Association website. This position paper will be presented at the 5th Edition of our **Free and Safe in Cyberspace**[35], held in Berlin on May 4th, 2018; a series conceived by such Association in 2015, focused on finding actionable answers to the challenges tackled by this paper.

1.13 The recent FBI/Symphony data escrow proposal

In recent months, while no NGOs, technology provider or nations have even proposed or really attempted to build technologies or certifications that can plausibly provide meaningiful cybersecurity in the face ever more widespread[3] and deeper critical vulnerabilities down to CPUs and manufacturing[36], calls for lawful access means keep coming every few month from from US and EU security agencies (often referred to as “backdoors”)

A joint call by the French and German Interior Ministers[37] for ways to ensure that no device is available in the market that prevents security agencies to “intervene” when legitimately authorized - echoing repeated calls from Obama and US agencies . More innovative proposals, while still very lacking in detail, have come from the FBI and the secure messaging company Symphony[38] for a solution based on voluntary third-party data escrow solutions, and from the announcement of “proposals under construction” by a number of widely-renowned and respected US cybersecurity experts[39].

Last January, for the 1st time since Snowden, the FBI has publicly endorsed - through its Director Wray[40] - a *specific* new key/data escrow solution or model as a best practice solution to solve the problems of *lawful hacking* and, implicitly, as alternative to state-mandated technical lawful access mechanisms. He referred to an agreement signed between secure messaging provider Symphony and New York State financial crime authorities that basically involves a third-party custodian entity deputed to hold logs of the data, and respond to the lawful access request. Here is what Director Wray had to say:

> *Some of you may know about the chat and messaging platform called Symphony. This was used by a group of major banks, and marketed as offering something called “guaranteed data deletion,” among other things. Maybe the labeling, maybe the content didn’t sit too well with the friendly regulator down the street—the New York Department of Financial Services. DFS was concerned that the feature could be used to hamper regulatory investigations of Wall Street. In response, the four banks reached an agreement with the Department to help ensure responsible use of Symphony. They agreed to keep a copy of all communications sent to or from them through Symphony for a period of seven years. The banks also agreed to store duplicate copies of the encryption keys for their messages with independent custodians who aren’t controlled by the banks.*
>
> *So at the end, the data in Symphony was still secure, still encrypted, but also accessible to the regulators so they could do their jobs. I’m confident that by working together and finding*

> *similar areas to agree and compromise, we can come up with solutions to the Going Dark problem.*

Though the information available is exceedingly scant, and very inadequate in its current form, we believe this FBI/Symphony model to be a **promising architectural approach** for ultra-secure systems, that could lead to transparently reconciling personal freedom and public safety, under certain scenarios and with very detailed and extreme safeguards.

1.14 Major downsides of the recent FBI/Symphony data escrow proposal

From the information publicly available about such *Symphony data escrow model*, there is no evidence whatsoever that the technical, socio-technical and governance safeguards and resilience provided by the third-party escrow agent (*custodian)* and by the offered Symphony IT service, provide the **ultra-high levels of transparency and trustworthiness** that would be needed to sufficiently mitigate great risks to both (1) the privacy of user of the IT service, by state agencies or criminals; as well as (2) the integrity and availability of the logs that are saved for future access of legitimately authorised investigations.

We suggest that a radically more detailed declination of this model could enable us to deliver meaningful IT security to all - while improving the effectiveness of cyber investigation - by ensuring that **both** the key/data escrow procedure, and the TC-compliant IT service itself, are subject to **transparency, accountability, oversight** and **security-review in relation to complexity**, that radically exceed state-of-the-art; on par with those that have been successfully applied to safeguard critical nuclear systems, best-of-breed paper-based elections processes or commercial aviation authorizations.

A nation may decide to **create new certifications** inspired by our Certification Body, but with different technical paradigms or different governance for example. Since even small details may fully compromise the level of trustworthiness, especially governance changes, then the Certification Body with publicly oppose any such plans and prospects.

A nation may decide to make only our Certification Body **mandatory for for all consumer and enterprise IT services**, regardless of their security level. For the reasons outlined about discussing the FBI/Symphony model, we'd be firmly against that.

2 Devil is in the Details

2.1 TRUSTLESS COMPUTING PARADIGMS

The Trustless Computing Paradigms define high-level binding requirements for future TC-compliant IT services. One in their final form, they are binding on the Certification Body, but can be amended by a super majority of the Certification Body Assembly.

They are intended to ensure and sustain highly resilient, profitable and open ecosystems for TC-compliant systems, initially for human communication and transaction, and gradually expand to other domains. They are not exhaustive, for the time being. They list the most critical guidelines which will be binding to future detailing of the certification requirements.

2.1.1 Trustless Computing Paradigms - Summary Version

(*this section is copied form section 1.6.2 above*)

A **TC-compliant IT service** will therefore be one which complies to all of the following:

1. *undergoes continuous certification by* an extremely **technically-proficient, comprehensive and citizen-accountable** independent standard-setting and certification body.
2. *assumes* that extremely-skilled attackers are willing to devote even **tens of millions of euros** to compromise its supply chain or lifecycle, through legal and illegal subversion of all kinds, including economic pressures; and advanced algorithmic, brute force and AI-assisted hacking.
3. *provides* extremely user-accountable and technically-proficient **oversight** of all hardware, software and organizational processes that *critically* involved in the entire lifecycle (i.e. including the supply chain). By "critical" we refer to hardware, software or procedures which cannot protect to a very high degree against confidentiality and integrity failures, or abuses, by using by implementing state-of-the-art time-proven OS, SoC and/or CPU level isolation/compartmentation techniques.
4. *provides* extreme levels of intensity, proficiency, ethical **security-review relative to system complexity** for all *critical* components;
5. *includes* only *critical* components that are publicly inspectable in their source designs, and strongly minimizes the use of non-Free/Open-source software and firmware, especially in critical components.
6. *includes* only highly-redundant and decentralized hardware and/or software **cryptosystems** whose protocols, algorithms and implementations are open, long-standing, extensively-verified and endorsed, and with substantial and "scalable" post-quantum resistance levels.
7. *includes* only innovations with **clear and low long-term royalty terms,** from patent and licensing, to prevent undue intellectual property right holders' pressures, lock-ins and vetoes; and sustainably ensure low-cost for affordability by average citizens;
8. *will* provide an **in-person offline key or data recovery function**, to benefit end-users, in case of loss of death or loss passcodes, and to enable a voluntary (i.e. in addition to current law requirements) compliance to legitimate lawful access requests. This function will rely on setups and management process of multiple hosting rooms in multiple jurisdictions that implement unprecedented safeguards. In addition to state-of-the-art security, these will utilize

only TC-compliant endpoints and door locking mechanism. Access to such rooms for any reason, always requires the express approval of an attorney and **5 trained citizen-jurors**, that are managed and accountable to the Certification Body - that will assess the compliance of the requests to national law, constitution and EU Charter of Human Rights. Any kind of remote access is physically disabled.

2.1.2 Trustless Computing Paradigms (Full Version)

A **TC-compliant IT service** will therefore be one which complies to all of the following:

A. AIMS: *aims* at ***constitutionally-meaningful*** **levels of actual and perceived trustworthiness** of the integrity and confidentiality (data and metadata), and not mere substantial improvements;

B. THREAT: *assumes* that extremely **skilled attackers are willing to devote even hundreds of millions** of dollars to compromise the lifecycle or supply chain through legal and illegal subversion of all kinds, including economic pressures; and many tens of thousands to compromise an individual end-user.

C. TRUSTLESSNESS. *assumes* an **active and complete lack of trust in anyone or anything, except** in the intrinsic constraints and incentives against decisive attacks to all organizational processes critically involved in the entire lifecycle, from standard setting to fabrication oversight, as assessable by any moderately informed and educated citizen.

D. OVERSIGHT: *provides* extremely user-accountable and technically-proficient **oversight** of all hardware, software and organizational processes *critically* involved in the entire lifecycle. "Critical" hereafter shall refer to hardware, software or procedures against whose possible vulnerabilities one can NOT be protected by using proven OS, SoC and/or CPU level isolation/ compartmentation techniques. This includes access for whatever reason to any server-side facilities or hosting rooms containing user-sensitive data.

E. SUPPLEMENTARITY: *aims* to provide a user-friendly **supplement or "add-on"** to ordinary commercial mobile and desktop devices, rather than a replacement to them.

F. ORGANIZATIONS: *provides* extreme user **citizen-accountability, independence and technical proficiency of all organizational processes critically involved** in the computing service lifecycle and operation, including the Certification Body itself. Involves direct and exhaustive involvement of informed samples of citizens in the design and operational security oversight of all critical components.

G. CRYPTO: ***includes*** **only highly-redundant hardware and/or software cryptosystems whose protocols, algorithms and implementations** are open, long-standing, standards-based and extensively verified and endorsed by recognized ethical security experts, and widely recognized for their post-quantum resistance levels aimed at post-quantum cryptography migration over the next 5-10 years. The above also applies to any use of zero-knowledge, **blockchain**, threshold cryptography, secret-sharing protocols.

H. INSPECTABILITY 1. *integrates and develops* only **software and firmware whose source code and compiler allows for inspecting without non-disclosure agreement** ("NDA"), and which is developed openly and publicly in all its iterations;

I. INSPECTABILITY 2. *includes* **only critical hardware components whose firmware (and microcode) and full hardware designs are publicly inspectable without NDA** at all times in open public structured format. In the case of processors, it will include code, hardware description source files (such as VHDL or Verilog files), Spin interpreter and similar, programming tools, and compilers;

J. INSPECTABILITY 3: *allows* for complete **hardware fabrication and assembly inspectability,** and extremely user-accountable and effective oversight, of all critical hardware components, in their critical manufacturing processes;

K. INSPECTABILITY 4: *ensures* availability of **one or more mirror physical copy of the complete server-side hosting room setups** to enable easy independent testing by anyone, while being charged only the marginal cost of providing such access; in addition to all needed service devices at marginal production cost.

L. *SECURITY-REVIEW. ensures* **extreme levels of highly-ethical highly-expert security-review relative to complexity**; i.e. extreme levels of intensity, competency, and "expected altruism" of engineering and security-review efforts - in relation to system complexity - for all *critical* software and hardware components; also by implementing extreme software and hardware compartmentation, and feature and performance minimization;

M. LICENSING. *strongly* ***minimizes*** **the inclusion of non-Free Software**, including updatable and non-updatable firmware. Makes extensive reuse of existing Free/Open Source Software components – through extreme stripping down, hardening and re-writing. It strongly aims at realising the computing system with the least amount of non-free software and firmware in security-critical hardware components;

N. TRAINING. *includes* **effective and exhaustive first-time in-person training for users**, to ensure knowledge of basic operational security (OpSec) and the risk management for self and others.

O. IP TERMS: *includes* **only technologies and innovations with clear and low long-term royalties** - from patenting and licensing fees - to prevent undue intellectual property right holders' pressures, lock-ins, patent vetoes, and ensure an open platform with sustainably low costs, affordable to most western citizens.

P. LEGAL*: ensures* that current cyber-security **legislations and state agencies practices** in the country of origin and/or localization of user, provider, assembly facilities, foundry - and other critical process involved - are <u>not</u> inconsistent with a constitutional, lawful and feasible compliance with these certifications; in regards to surveillance, mandatory encryption key disclosure, crypto exports, liability, and other relevant legislations.

Q. ASSEMBLY. *provides* one or more dedicated crowded urban street-level glass-walled spaces where devices are publicly assembled, verified, flashed, and transferred to their users. It will be subject to 24/7 high-trustworthiness live streaming oversight, and monitoring.

R. LIABILITY: *includes* an extreme level of **cumulative liability, contractual/economic and legal,** for all individuals and organizations critically involved for not strictly following procedures or willingly compromising the life-cycle.

S. OPEN ECOSYSTEM. *involves* participants to an initial open R&D Consortium, which will set out to build the first certified service, that **commit to terms that ensures very-high resilience to the openness of the ecosystem** and its resistance to economic pressures, including: (a) through such consortium, offer only certified services; (b) state clear, perpetual and very-low (or null) royalties to all the IP they integrated and developed in the services they offer jointly or independently.

T. INTEGRITY: *shall* provide a uniquely accountable and "trustless" form of *remote attestation,* in addition to extreme *anti-tampering,* in order to further guarantee a user that its interlocutors' devices have not been insecurely modified. (For example, the entire local archive of a highly-private mailing list of frontline political activist group, or of top executives of a corporation, may be totally jeopardized if only one of their interlocutors applies the wrong software modification). Nevertheless, users and researchers must be able to fully reprogram the software, after triggering the tampering detection mechanism that warns all other users, to facilitate open research.

U. SERVER-SIDE & DATA RECOVERY. *will* provide extreme safeguards for all security- and privacy-sensitive server-side (and/or "decentralized") infrastructure - which **will mandatorily include the provision of in-person offline user key and data recovery,** for benefit end-users - in case of loss of death or loss passcodes - and to enable a voluntary (i.e. in addition to current law requirements) compliance to only legitimate and constitutional lawful access requests. Deploys only TC-compliant **endpoints and *networks*** for any critical server-side endpoints involved in the server-side/decentralized components and complaint **hosting room access management setups and processes**, *TrustlessRooms,* that are standardized and certified by the Certification Body. These collectively will comply to the following safeguards:

  a. *Shall* physically disable remote admin access, and physical access by anyone will be conditional to the **physical presence and express approval of at least 5 randomly-selected citizen-jurors** - in addition to an attorney, and 2 system administrators - through dedicated TC-complaint access mechanism (such a keypads). Citizen-witnesses are entitled to record anything and ask for a dump of all code before and after any session. Citizen-jurors are managed and regulated by the Certification Body to ensure their adequate vetting, self-training, resilient and protection;

  b. *Shall* use *secret sharing* cryptographic techniques, threshold cryptography, or other similar advanced but time-tested protocols — in addition to such offline authorization procedures – to enable 10 or more citizen-witnesses participating through via video stream to also approve using TC-compliant client devices; therefore adding an additional layer of security.

  c. *Shall* enable security-review in one or more complete replicas, including *TrustlessRooms* for verification by anyone who might substantiate even a low to moderate capacity to do so;

  d. *Shall* employ state-of-the-art public video streaming and recording, and shall be located at street level in busy urban streets, with large glass fronts, to increase perceived social control and trustworthiness.

  e. *Shall* maintain copies of time-limited encryption keys of subsets of data or metadata of users (and for each user *personas* if multiple ones) by providing socio-technical systems with extremely-careful safeguards to enable the highest user-control and security in data recovery in the scenarios of user death or user loss of password, as well as **enabling lawful access that is lawful, constitutional and compliant with *EU Charter of Human Right.*** It will allow for voluntary compliance (i.e. in addition to what is required by all relevant laws) to limited and targeted due- process lawful access requests, with the extremely-careful safeguards that follow:

i. *Shall* enable the *TrustlessRoom* citizen-jurors to launch a “***Scorched earth procedure***” with plausible deniability, which allows a qualified majority of such citizen-jurors – in cases of extreme abuse attempts – to cause an immediate physical destruction of all sensitive keys and data in the *TrustlessRoom*, which will remains available in other *TrustlessRooms* of the same provider in a different country. Providers that are governmental agencies, civilian or military, and offer service only to public employees are exempt, transparently to their users, from the requirements of this clause.

ii. *Shall* be offered only after the service has been used successfully tested for 3 months, in publicly-accessible pilot deployments, with real data, that involve highly-sensitive communications by voluntary elected public officials, as well as by highly expert ethical hackers. (Use of such systems by elected officials would in fact make so that their communications are, on one side, much more resistant to to undetected illegal espionage and blackmail, while on the other, are interceptable when mandated by a court warrant.)

iii. *Shall* offer the service only where at least 3 *TrustlessRooms* are located in at least 3 different nations. All encryption keys of all security- and privacy-sensitive data will be shared between the 3 *TrustlessRooms*, so that even if, through unconstitutional or illegal action, attackers prevail in one nation, they would only have one third of the keys required, unless they prevail also in the other two countries. Eligible nations will be such that:

    1. the service can be offered as a service that is not subject to state mandatory lawful intercept or access legislation (such as those typical of phone operators under US CALEA);
    2. mandatory key disclosure, and other legislation, or known practices, do NOT make it illegal - except with negligible consequences - to withhold access (with or without gag order) to warrant-based or state-security-based government requests, that may be believed by involved *citizen-jury-like* body
    3. liability for malicious or gravely negligent breach the laws or regulations are substantial - and proportionate to the damage caused - for all citizen-witnesses, citizen-jurors, provider staff or for attackers (both state and non-state actors).
    4. at least one of those nations is not part of the same first degree military or Intelligence/Surveillance alliances (Five eyes, Nato, EU, etc.);
    5. when and if a nation no longer complies with conditions (1) to (4) above, then the Provider must give a choice to each individual user to agree to transfer such services to a *TrustlessRoom* in another nation, or terminate his/her service by recuperating all his data.

iv. *Shall* have a technological limit in the maximum number of users, and percentage of total users, whose personal data or keys may be extracted within a given time frame;

v. *Shall* utilize the highest precautions to (a) prevent or minimize leakage of non-public information related to the lawful access requests, through video and other oversight processes; and (b) to prevent the accidental or malicious deletion or alteration of stored user data, keys and logs, also by integrating time-proven state-of-the-art **blockchain** technologies.

V. FABRICATION. *ensures* that all *critical* Integrated Circuits (such as CPU, SoC, memory, etc) components and critical assembly processes are executed under a *TrustlessSite* process whereby:

a. *aims* to substantially or radically exceed in end-user-assurance those of Common Criteria Site Certification EAL 5 and *NSA Trusted Foundry Program*, at substantially lower costs.

b. *setup and configure* an **extensive sensing, and monitoring infrastructure** and allow about 3 (or more) competent, trained, redundant and technicians to verify thoroughly all the critical steps, from the monitoring room and/or inside the cleanroom.

c. *utilizes* equipment and sensors, that as much as possible not require direct interventions or disruption of the foundry equipment and facilities, but just rely on setting up an additional overlay of sensing equipment, and on getting copy of the existing quality control sensor feeds. This would also increase the portability of the TrustlessSite processes to other foundries, and therefore increase its resiliency.

d. *utilizes* only foundries, (such as Lfoundry, Italy) that allow the technicians and **5 citizen-witnesses** (or peer-witness for governmental/military Provider) to thoroughly oversee and monitor all critical processes - even though that may force the utilization of older foundries with technologies and simpler processes and less IP.

2.2 Main concepts and breakthroughs

We re-conceptualize IT trustworthiness as exclusively a *cyber-social* problem, and not a technical one. Of course, the technical quality and innovations of all components in algorithms, software, protocols, hardware and fabrication processes determine the cybersecurity of an IT system, but the likelihood of their occurrence, and their availability to law-abiding actors rather than non law-abiding actors, is all a matter of governance.

We redefine cybersecurity as a **by-product** of the **intrinsic resilience, accountability and technical proficiency** and organizational processes - such as supply chain, human processes, standard setting - that are critically involved in the entire life-cycle of producing and consuming an IT product.

Once we do that, cybersecurity and trustworthiness are, in fact, a *governance* problem with a combination of technologies, regulations, economic (dis)incentives and social norms. Achieving trustworthiness by being ***trustless*** will require uncompromisingly applying best-of-breed "*zero trust*" social and technical paradigms from different fields, including:

- **cyber-social principles of highest-trustworthiness** military IT and civil aviation systems, such as secret sharing, threshold cryptography, blockchain and zero-knowledge protocols for cryptography and human process protocols.
- **citizen-witness, citizen jury and voting-booth** organizational procedures in democratic elections, and
- organizational constituent processes, and statutory architectures, aimed at **extreme transparency, user/citizen-accountability and technical-proficiency.**

We propose that the trustworthiness of any IT service should not be assessed according to reputation or compliance of part of its critical components to **insufficiently comprehensive and self-referential** certification standards, as it is done today through the dominant "trusted computing" model. Rather it must be measured through a fine-grained continuous modeling and real-time transparent monitoring of all relevant and intrinsic technological and procedural constraints and all relevant organizational, economic, liability, legal and sociobehavioral disincentives, that might cause critically-involved individuals and organizations to perform unexpected compromising actions.

It is therefore necessary that "so called" **security-by-design** paradigms be brought to their ultimate conclusion, by requiring that IT services be `*trustless*`, i.e., **devoid of the need or assumption of unverified trust** in anyone or anything, except in quality the inherent self-guaranteeing quality and accountability of the organizational processes, that critically underlie all critical lifecycle components, and whose quality is recognizable by moderately informed and educated citizens.

To that end we propose the Certification Body and its initial statutes, by-laws and high-level binding guidelines embedded in the Trustless Computing Paradigms (or "Paradigm") to achieve and sustain actual and perceived levels of trustworthiness of IT systems that are today largely deemed impossible, inconceivable or uneconomical, and ensure its wide adoption and affordability by all.

Governance is about constituent processes. The sustainability in time of the democratic and technical quality of such governance is ultimately wholly dependent on the foreseeable ability of the initial organizational statutes, and members of initial key governing boards, to maximize the chances of self-improvement, amidst the pressures of growth and success, because *"**One cannot in the nature of things expect a little tree that has been turned into a club to put forth leaves**"*, **s**aid Martin Buber.

The trustworthiness of any end-to-end IT service or experience will not be assessed according to organizational cognitive trust (reputation) and compliance to gravely incomplete and auto-referential certifications standards (e.g. Common Criteria, FIPS, Trusted Computing), as done today. Rather, cybersecurity will be assessed and certified as the level of trustworthiness that individuals and organizations critically-involved will not perform unexpected actions, and shall be derived from dynamically modeling all technological, procedural and statute cyber-social intrinsic constraints, and all organizational, economic, liability, legal and social disincentives, that are foreseeable at any given time.

2.3 Scope and Definition of Trustless Computing

Today, IT systems that provide the highest level of trustworthiness are referred to as *high-trustworthiness*; these are used mainly in business or national security contexts. But even such levels have been proven by recent revelations and reported security breaches to be highly inadequate for the most critical IT use cases involving both high-value targets as well as ordinary citizens.

While perfect trustworthiness is impossible, it is crucial to set an arbitrary yet measurable level of target trustworthiness for IT communications of confidentiality, authenticity, integrity and nonrepudiation - which we define as “ultra-high trustworthiness IT” - which are sufficiently resistant to wide-spread compromisation to promote the retention or increase of the levels of freedom and democracy in society, and individuals communication rights. It should enable citizens’ responsible and effective Internet-connected exercise of their communication civil rights, in accordance to international human rights agreement such as the *EU Charter of Fundamental Rights,* except for remote voting in governmental elections. We talk about IT *services*, when talking about IT that are *high-trustworthiness* or beyond, because all IT *products* and *systems* ultimately necessarily rely critically on at least some services after initial sale or deployment, such as software upgrades, and more.

We talk about IT service *lifecycle* since the trustworthiness of a service is completely dependent on the trustworthiness levels of lifecycle of any and all of its critical technical and organizational components; from standardization to fabrication oversight, to critical server-side facilities access, to critical systems development tools.

Definition of *ultra-high trustworthiness IT*: An IT service that we can confidently predict to be able to resist persistent attempts - by actors with high plausible deniability and very low actual accountability - to critically and persistently compromise (A) its life-cycle, continuously, through investments of even tens of millions of euros and (B) a single user of the service, through investments of tens of thousands (such as those associated with enacting such level of abuse through on-site, proximity-based user surveillance, or non-scalable remote endpoint techniques, such as NSA TAO).

Definition of *Trustless Computing:* An *ultra-high trustworthiness IT* service whose respect of human rights conventions such as the *EU Charter of Fundamental Rights* does not require the need or assumption of trust in any item or any standard, except in the intrinsic resistance to abuse of the organizational processes critically involved, as recognizable by moderately informed and educated citizens. We mean “trustless” in its primary literal meaning of “untrusting” and “distrustful”, i.e. lacking any need for or assumption of trust in anything and anyone. While ultra-high trustworthiness IT concerns the trustworthiness towards the user of a given IT service or experience, Trustless Computing refers to its trustworthiness both towards the user, as well as its “trustworthiness” towards society, in so far as it reasonably protects society from abuse by the user to hide and plan crimes. The concept adds the requirement of compliance, by the provider, or, execution by the state, of constitutional - no more no less - lawful access mandates.

2.4 Role of Free Software and open innovation concepts.

Free/Open Source Software, while providing important civil freedom, does not directly improve trustworthiness of a software in comparison to that whose source code is merely publicly-verifiable without NDA. On the contrary, at times it has constrained viable business models, and therefore reduced resources available for adequate security-review relative to complexity. Nonetheless, the project will very strictly mandate Free/Open Source Software and firmware, with little exception for non-critical parts, because it strongly promotes incentives for open innovation communities, volunteer expert security-review and overall ecosystem governance decentralisation, which in turn substantially contributes to IT actual and perceived security, and promotes an ecosystem that is highly-resilient to short- and long-term changing technological, legislative and societal contexts. Without the very active and well meaning participation (paid and not paid) of many of the world-best IT security experts and “communities”, it would be unlikely to achieve the necessary security-review intensity and quality, relative to complexity, that is needed to achieve the project aims.

Without the very active participation (paid and not paid) of the world-best IT security experts and “community”, it would be unlikely that a project even with over 100M€ budget could have reasonable expectations to prevent successful remote attacks from the numerous and varied entities with access to remote vulnerabilities devised, commissioned, acquired, purchased or discovered, to date and in the future, by entities that are extremely well-financed and have unprecedented accumulated skill-sets.

Over the last thirty years, a huge amount of volunteer and paid work has been devoted to developing Free Software with the aim of promoting users' civil freedom in computing. But, to date, no end-user computing device available at any cost which would give the user meaningful confidence that its computing is not completely compromised undetectably at a low marginal cost and risk. No end-user device available today that does NOT contain at least some "critical" software/firmware components that are not nearly sufficiently verified relative to complexity, or (b) are non-verifiable in its source code (without NDA) or even proprietary.

Free/Open Source Software, while providing some civil freedoms, does not *directly* improve trustworthiness of a software application or stack, in comparison to that whose source code is merely publicly-verifiable without NDA. At times, on the contrary, it has constrained available business models in ways that prevented the sustainable attraction of the very large resources necessary to guarantee a sufficiently-extreme security-review relative to complexity.

Nonetheless, an adequate new standard may need to very strictly mandate Free/Open Source Software and firmware, with few and/or temporary exceptions for non-critical parts, because it strongly promotes incentives for open innovation communities, volunteer expert security-review and overall ecosystem governance decentralisation.

These, in turn, substantially contribute to IT actual and perceived security, and promotes an ecosystem that is highly-resilient to very strong economic pressures, as well as short- and long-term changing technological, legislative and societal contexts.

Most importantly, **without the very active and well meaning participation (paid and not paid) of many of the world-best IT security experts and “communities”, it would be unlikely to achieve a sufficiently-extreme necessary security-review intensity and quality, relative to complexity that is needed** to achieve the project aims. Without such participation, it would be unlikely that a project even with a budget of over hundreds of millions of euros could have reasonable expectations to prevent successful remote attacks from the numerous and varied entities, which have access to remote vulnerabilities that are regularly devised, commissioned, acquired, purchased or discovered, by entities that are extremely well-financed, have unprecedented accumulated skill-sets and often low or inexistent actual liability.

2.5 Fabrication Phase: Safeguarding against attacks during fabrication of critical integrated circuits and assembly

Fabrication and design phases of all *critical* TC-compliant hardware components will be subject to oversight processes, or TrustlessSite, that aims to substantially exceed in trustworthiness those of even Common Criteria EAL5-7 and *NSA Trusted Foundry Program*, at substantially lower costs. Trustless Computing Site Certification (or *TrustlessSite*) oversight processes for all critical phases (which cannot economically be verified ex-post) will involve extreme safeguards, including using only TC-compliant device for critical functions, and including on-site offline oversight of 5 randomly-selected trained citizen-witnesses, similar to polling station processes in governmental elections.

Why is the *TrustlessSite* needed and cost-effective?

Trustless Site Certification processes are needed because of the grave and real risk that hardware or software vulnerabilities may be introduced by some entity during the manufacturing process[41], and inadequacy of current fabrication standards. Such introduction, if performed in critical fabrications phases, cannot be ascertained afterwards. **"*Trust cannot be added to integrated circuits after fabrication*"**[42] said the US Defense Science Board already in 2005. At first, it would appear that building a chip manufacturing plant would be the best way to provide the highest security of the chip manufacturing process. However, at a cost of 200M€, for very old technology, to 4bn€, for the latest, such costs are not only prohibitive but of very little use since, even though such plant may be located in the same nation where the TC-complaint service is offered, the problem of verifying and overseeing the process remains almost completely intact. Therefore, even if there was a budget of over 100M€ available to ensure hardware security, the best way to spend such budget would be in oversight procedures and technologies rather than manufacturing, provided that the necessary foundry access is granted.

How it works.

Follows possible solution, for the sake of validating its feasibility. The actual solution will be developed during the project. *TrustlessSite* will deploy general concepts reportedly applied by *NSA Trusted Access/Foundry Program* today in cases in which they require the highest-level fabrication oversight trustworthiness. They reportedly choose a foundry that fits the equipment and general oversight process specifications - located, if not in the US, in a country that overall provide more trustworthiness than others - which will agree to:

- (1) Make sure that the requested hardware is all produced in one continuous batch in a short time span (a few days or weeks), as is typical anyway;
- (2) Allow, for each batch, to setup and configure an extensive sensing, and monitoring infrastructure - often made by specialized proprietary companies - and allow about 3 (or more) competent, trained, redundant and trusted technicians, per shift, to verify thoroughly the entire process, 24/7 and on-site, from the monitoring room and inside the cleanroom.

In addition to that, the Trustless Site Certification will:

- (A) Add at minimum number "user witnesses", made up of 5 (or more) randomly-sampled Trustless users and 4 (or more) user-elected Trustless users, in a role of active oversight witnesses 24/7. They would be well paid to take that time off, would be extensively trained and "self trained" through open participatory processes;
- (B) produce *critical* ICs (such as CPU, SoC, memory, etc) at EU-based 200-300mm EAL5+ foundries with older technologies, simpler processes, and less third-party IP obstacles than today's' Asian mega fabs, that allow the technicians and witnesses to publicly and completely document the process with videos, photos and more. One such foundry, Lfoundry, has already agreed to the access and transparency terms outlined here, and to its economic and IP breach feasibility, as participant of previous R&D proposals.
- (C) Equipment and sensors, to be applied to the chosen foundries, should as much as possible not require direct interventions or disruption of the foundry equipment and facilities, but just rely on setting up an additional overlay of sensing equipment, and on getting copy of the

existing quality control sensor feeds. This would also increase the “portability” of the *TrustlessSite* processes to other foundries, and in part the resiliency of the solution.

- (D) Sensing and oversight equipment will as much as possible be air gapped, make use of high trustworthiness inspectable systems, and as much possible TC-compliant.

2.6 Citizen-witness and Citizen-jury processes to secure IT and other critical systems

Revolutionary socio-technical processes, including based on citizen-witness procedures - such as those use in voting-booths in governmental elections - will be devised to radically increase safeguard that critical processes in the life-cycle of complex and critical systems happen as expected, such as those for physical access to critical server room or oversight of critical ICs fabrication.

Recent examples and proposals indicate the potential of such procedures in ICT. In a recent video Bruce Schneier suggests use of citizen witnesses for the oversight of critical ICT life-cycle phases[43].A similar rationale inspired NSA introduction of a “2-man rule” for access to hosting rooms[44] to prevent a future Snowden leak; (c) A 2-man cockpit rule was announced in 2017 by various European airlines following a airline crash caused by a pilot suicide [45];

The Brazilian state IT agency SERPRO has internal regulations that intrinsically requires 4 state officials of 4 different public agencies need to be physically[46] present at a specific hosting room and consent in order to allow access to the emails of a state employee based on a court order. More recently, they are increasing the trustworthiness of their solution[47] for both citizens and law enforcement on the server side with additional safeguards, through Kryptus solutions. Such an approach, however, still does not deal adequately with the trustworthiness of several other potential vulnerabilities in the life-cycle, such as: client devices HW and SW, other critical SW and HW stack on the server side, the systems use by law enforcement to manipulate and store the acquired info, hardware fabrication of critical HW components.

Current procedures for lawful access to a user’s keys in Austrian for digital passports[48] currently require 3 officials from different state agencies in a a sort of in-person secret-sharing and “threshold secret” processes. In respect to such process, the TCCB Paradigms we add much higher and more comprehensive technical security requirements and - given the low citizens’ trust in governments - citizen-witnesses or citizen-juries processes would be added to the presence of officials from different state agencies, in order to add an additional layer of guarantee for end-users.

2.7 Fostering an open computing base and ecosystem

Together with the parallel establishment of spin-off startup and a foundation - comprised of technical, end-user and commercialization members - the Certification Body will create and sustain highly-competent and user-accountable computing standards, a **profitable ecosystem of independent service providers**, and **an active expert ethical hacking community**, around the creation and decentralized evolution of the **world’s most user-trustworthy general-purpose computing services platform, lifecycle, and certifications**.

The objectives of the Certification Body and Association will be to:

- (A) Realize standards for end-to-end computing services delivering **ultra-high levels of trustworthiness** in confidentiality and integrity that are compatible with a justified confidence in a meaningful protection from remote abuse of users' constitutional communication rights. These should allow users and service providers to achieve and sustain actual and perceived levels of trustworthiness of IT systems that are today largely deemed impossible, inconceivable or uneconomical, and to ensure its wide adoption by millions and its ultimate affordability to any citizen no later than three years, albeit through minimal initial features and performance -- these will initially mean to complement, and not replace, a typical user's everyday desktop or mobile computing.
- (B) Enable any willing service provider to offer such computing services, creating a **highly-decentralized and participatory ecosystem** of organizations, whose technical and user-accountability effectiveness is highly-resilient to advanced persistent threats along short- and long-term changing technological, legislative and societal contexts. They will provide checks and balances among different user-accountable organizations, effective organization re-constituent processes, autonomous communities of self-provisioning users, competing service providers, and even competing standards organizations.

2.8 Relation to international civil rights frameworks

Constitutionally-meaningful **confidentiality and integrity** of digital data, and the **preservation of effective cyber-investigation capabilities**, are not, as most believe, an "either/or" choice, but a "both or neither" challenge. In fact, neither digital confidentiality nor effective cyber-investigation capabilities are available today because nearly all IT services - including cyber-investigation tools - can be compromised at scale through vulnerabilities that even mid-level criminal entities and powerful nations have directly implanted or indirectly sanctioned - by hugely financing the market for critical vulnerabilities, by deliberately subverting key lifecycle phases, by neither disclosing nor properly safeguarding found vulnerabilities, and by deliberately promoting broken standards.

While **perfect trustworthiness is impossible**, it is crucial to set a measurable level of target trustworthiness in confidentiality and integrity of IT services, which are sufficiently resistant to being compromised at scale, in order to substantially increase the levels of freedom and democracy in the society. Such levels should at least enable citizens to responsibly and effectively exercise their internet-connected communication civil rights, in accordance to international human rights agreements such as the **UN Charter** and the EU Charter of Fundamental Rights, except for remote voting in governmental elections and political primaries.

Ultimately, it is a "**both or neither**" challenge because, to a very large extent, the extreme technical, cyber-social and organizational *safeguards* that are needed to ensure *ultra*-high levels of trustworthiness of communications, are the same safeguards that are needed to define innovative lawful access compliance protocols and certifications which will reduce the risks of widespread abuse of the civil rights of citizens AND of integrity of cyber investigations to levels that are (a) compatible with the **EU Charter of Human Rights**, and (b) substantially or radically less prone to abuse than all currently available alternatives.

2.9 Radical mitigation of potential criminal abuse of publicly-available ultra-secure IT system designs

The public verifiability of the source designs of every critical software & hardware component as prescribed by the Trustless Computing paradigms could appear to potentially enable malevolent actors to fabricate their own devices beyond the capability of interception by even the most powerful intelligence. In fact, several large non-EU non-NATO non-allied countries already have all the capabilities to build systems to the Trustless trustworthiness levels, and could make it available to malevolent actors. Nonetheless, we have carefully concocted preliminary definitions of safeguards to sufficiently and radically mitigate such a threat.

In theory, smaller potentially malevolent states or groups, by contrast, in order to achieve and sustain the Trustless levels of trustworthiness, would need to have an extreme control of a suitable semiconductor foundry, because, as US Defense Science Board said back in 2005, ***"Trust cannot be added to integrated circuits after fabrication*"**[49]. The dramatic increase in the complexity of critical HW fabrication and design processes makes avoiding the insertion of an undetectable critical vulnerability throughout the supply chain and lifecycle an easy task. Furthermore, even a small foundry, by current global standards, is a highly complex operation with a staff of over 1000 and typically 800 or more discrete fabrication processes over several weeks, including dozens of critical ones where an error or malicious modification, can not be detected afterwards. Provisions will be set in the HW/SW architecture to ensure that TC-compliant endpoint devices cannot be produced in smaller prototyping labs, mainly through the use of IP cores tied to specific, capital intensive fabrication processes, naturally not available on mini-scale prototyping fabrication facilities and foundries.

Furthermore, fabrication oversight procedures are needed because of the grave and real risk that hardware vulnerabilities may be introduced by some entity during the manufacturing process, and inadequacy of current fabrication standards. Such introduction, if performed in critical fabrications phases, cannot be ascertained afterwards. At first, it would appear that building a chip manufacturing plant would be the best way to provide the highest security of the chip manufacturing process.

However, at a cost of hundreds of millions of dollars, for very old technology, to billions of dollars, for the latest, such costs are not only prohibitive but of very little use since, even though such plant may be located in the same nation where the compliant service is offered, the problem of verifying and overseeing the process remains almost completely intact. Therefore, even if there was a budget of over $100M available to ensure hardware security, the best way to spend such budget would be in oversight procedures and technologies rather than manufacturing, provided that the necessary foundry access is granted.

In the rare case in which a malevolent foreign terrorist entity (state or non-state supported) might attempt to enter into agreements with suitable foundries in non-democratic or highly unstable nations to build such systems, security agencies of nations participating in TCCB or allied could quite easily make sure to either prevent it or, better yet, enact intelligence operations aimed at inserting vulnerabilities in their fabrication or design processes to acquire in the future highly valuable intelligence

To the extent that the above mentioned safeguards may prove to be insufficient to adequately mitigate such risks, TCCB may explore the possibility that a subset of the hardware designs - as opposed to all other critical technical components - may not be made publicly inspectable in their source design, but subject to multiple redundant verifications which involve direct oversight processes involving both randomly sampled citizens and state officials, under suitably controlled environments.

2.10 Extending TCCB to other critical societal systems

While initially aimed at human communications and transaction, TCCB will expand to other domains where integrity and/or confidentiality are of the utmost important, and to others where availability (such as safety critical, tactical communications) is crucial.

2.10.1 Targeted lawful access programs

Some of the leading US/UK IT security experts that have been for decades the most staunch opposers of lawful access solution for IP communications, acknowledge that some "going dark" problem exists or could potentially exist and that - regardless of varying opinions about its severity - a solution will need to be found as political pressures will keep mounting to retain. They see that solution in a formalization, expansion and transparent (or translucent) regulation and oversight of *lawful hacking*.

Three of the most prominent among the 14 experts mentioned above, and Sandy Clark, have proposed - in 2 foundational reports of 2013 "*Going Bright: Wiretapping without Weakening Communications Infrastructure"* report[50] and of 2014 *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet[51]* ("*Lawful Hacking report*" below) - an alternative solution to the problem. It requires the state to *"exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders",* and properly regulate it. It basically proposes to formalize and strictly regulate the state's ability to hack citizens pursuant a court order. It proposes very extensive measures and safeguards to mitigate the consequent negative effects, including:

A. Creation of new vulnerabilities is not allowed, but only discovery and creation of ways to exploit for existing vulnerabilities.

B. Mandatory reporting of vulnerabilities to IT vendors on discovery or acquisition, with some exceptions. It counts on the fact that new will be found and that it takes time for vulnerabilities to be patched;

C. Limitation of lawful access software to only authorized access actions (whether intercept, search, or else).

They proposed to formalize and regulate the use of "lawful cracking" techniques as a way to enable the state to pursue cyber-investigation:

> *"We propose an alternative to the FBI's proposal: Instead of building wiretapping capabilities into communications infrastructure and applications, government wiretappers can behave like the bad guys. That is, they can exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders.*
> *We are not advocating the creation of new security holes, but rather observing that exploiting those that already exist represents a viable—and significantly better—alternative to the FBI's proposals for mandating infrastructure insecurity. Put simply, the choice is between formalizing (and thereby constraining) the ability of law enforcement to occasionally use existing security vulnerabilities—something the FBI and other law enforcement agencies already do when necessary without much public or legal scrutiny or living with those*

> *vulnerabilities and intentionally and systematically creating a set of predictable new vulnerabilities that despite best efforts will be exploitable by everyone."*

Formalizing and regulating such *lawful hacking*, or better "*lawful cracking*" - as suggested by the *Lawful Hacking report* - would be a substantial improvement in respect to the status quo, if done right. Their recommendations would provide resilient and insightful technical requirements to radically raise the trustworthiness of lawful cracking tools of *lawful access* systems. They focus on identifying mitigations to reduce a much as possible risk of abuse. It could also inspire current international voluntary standards for such systems, such as those currently maintained by ETSI in Europe and NIST in the US, or, better, new better bodies.

But given their inherent limitation - as highlighted by leading German researchers like Sven Herpig[52] - we believe such suggestions should be framed differently for ordinary commercial systems as opposed for high-trustworthiness systems.

For ordinary commercial systems, on the one hand, such mitigations, although only partially effective, seem nonetheless acceptable for ordinary commercial systems (i.e. low and medium-trustworthiness systems), as they would not change significantly the overall vulnerability of such systems. In fact, such systems' ratio of security review relative to complexity - and low or ineffective HW/SW systems compartmentation - will expectedly remain so low, as to guarantee state availability of at least one critical vulnerability, that enables full undetected remote endpoint comprimization. In lay terms, having 10 or 5 holes would not affect significantly the number of actors with access to at least one critical remote vulnerability.

For high-trustworthiness systems, on the other hand, making it illegal for the state to create new vulnerabilities would in theory benefit the wide availability of *IT systems of meaningfully high-trustworthiness levels*. However, it is very unlikely that a law in that regard will ever be approved and enforced. In fact, it seems highly unlikely that powerful states would reliably enforce, with serious liability, an outlawing of the creation, purchase, discovery or use of new undisclosed vulnerabilities, as it would objectively put them at disadvantage towards other state and non-state actors that would continue doing so, through (relatively) symmetric or (relatively) asymmetric vulnerabilities.

As in the US, increasingly in Europe and in Germany there is much contradictions with large and announcements to make national IT systems radically more secure, and larger ones deputed on the contrary to break much of the same systems, such as the new German Zitis 400-strong force. As the Cyber Security Council Germany writes "*When talking about an 'Agency for Disruptive Innovations in Cybersecurity and Key Technologies' (ADIC), one must ask oneself how such an actor is not in competition with other authorities such as the Central Information Security Authority (ZITiS)."* [53]

And their effort would obviously focus on those systems to which they do not have access to yet, i.e. high-trustworthiness IT systems. Therefore, state and non-state pressures on breaking the life-cycle of high-trustworthiness systems would likely remain or increase, as would the current lack of standards for systems for both citizen communications and lawful access schemes.

In fact, the *Lawful Hacking report* does not specify sufficiently-extreme organizational and technical generic IT security requirements for the entire life-cycle of the critically involved HW, SW and organizational components.

POLICY RECOMMENDATION. So therefore, while this paper is outlining a proposal that is independent of any policy changes, we nevertheless provide below some policy suggestions - to democratic nations in general - in regards to TCCB and related matters:

A. We propose to adopt and extend the recommendations for lawful hacking systems and programs contained in the *Lawful Hacking report* by also:

   a. Requiring sufficiently-extreme organizational and technical generic IT security requirements for the entire life-cycle of the critically involved HW, SW and organizational components, which would be in addition to those specific to lawful hacking *lawful access* safeguards specified in the mentioned proposal.

   b. Mandating or incentivizing certification of *lawful access* services, including lawful hacking, as well as for IT systems in all e-government critical use case scenarios, by approved international bodies with a very-high level of technical-proficiency, ethical standing and citizen-accountability, such as TCCB.

   c. Forbidding any governmental agent or agency - strongly enforced through severe sanctions - to create, purchase or maintain hidden new vulnerabilities in systems that are compliant to TCCB, since they enact a voluntary cyber-social service to respond to lawful access requests, as described above. Mandate the immediate disclosure to the Provider of any vulnerabilities or weaknesses that are discovered.

   d. In the USA, in particular, additional policy changes are proposed, and would be required in order for TC-compliant IT service to certifiable when either the provider or server-side facilities are located there:

      i. The Vulnerabilities Equities Process of the ODNI[1] should amended to comply to point c. above.

      ii. National Security Letters, and related gag orders, should not be applicable to systems similar to TC-compliant IT service, since they enact a reliable voluntary cyber-social service to timely respond to lawful access requests for national security matters.

      iii. Other legislative changes that may be required to make the lawful access request compliance processes of the *TrustlessRoom* above possible, without legal risks for the involved "citizen-jurors" for legal consequences of their refusal to comply, by majority, on the basis or rational articulable motivations of unconstitutionality.

B. Promote the creation and wide-market, though voluntary adoption, of TCCB.

C. Promote the creation of initial open-licensed TC-compliant ecosystem spanning the entire life-cycle computing experience.

2.10.2 Bulk lawful access systems

[1] https://www.eff.org/deeplinks/2015/03/government-says-it-has-policy-disclosing-zero-days-where-are-documents-prove-it

Many EU states, legally, filter Internet traffic in order to spot keywords combinations that could be a sign of criminal activity. As for Germany, *"Every year the parliamentary control committee issues a brief, general report on surveillance activities. The report for the year 2010 received a lot of attention in the media because it stated that automatic searches with more than 15,000 keywords identified over 37 million telecommunications, mostly emails, for further examination"[54].* That's one of many EU legal, but dubiously constitutional, bulk surveillance state programs.

Regardless of one's opinion as to whether such processes should or should not be legally authorized or mandated, everyone will agree that it is crucial that such systems should not be abused through unauthorized manual access or unknown vulnerabilities. Given the current standards for such systems through technical or organizational vulnerabilities, these could be abuses by agencies or agents to target individuals that do not strictly fit the legally sanctioned keyword parameters.

We are inspired by the systems and processes proposed and tested by NSA top engineer and whistleblower **Bill Binney** with ThinThread[55], before it was turned into the PRISM system. It aimed to ensure that flagging for suspicious traffic would be done by legal due process and agreed upon parameters, rather than at the whim of agency staff. Its proposal, however, did not provide for ways to ensure such accountability at the low-level IT systems on which Thin Thread relied and still relies.

A TC-compliant system could be deployed (or even mandated by law) so as to provide a **fully–automated keyword search of leads to possible criminal activity**, in such a way that manual interference or abuse is radically mitigated. It would provide the user-verifiability of the fact that communications identified for manual "further examination" are created exclusively through democratically-approved and transparent parameters, rather than changing discretional factors or manual choice. It would produce a win-win situation in which suspicious communication patterns could be identified, while completely preserving the privacy of innocent citizens which are not under reasonable suspicions.

In the future, some of such searches might happen through homomorphic cryptography. "Encrypted Search" might be deployed, which allows for arbitrary queries to an encrypted data set so that after "discovering" that something matches a certain criteria set, state agencies could request access to the very specific data.

Such functionality would allow for the full capability of analyzing all communications for suspicious activity without the huge risk of abuse and arbitrariness of a manual, or unaccountable process, as well explained by Prof. Lawrence Lessig[56]. It would radically promote both privacy and security by concurrently fulfilling both the great utility for security agencies to apply the latest big data analysis techniques to help identify suspected criminal activity, and protect the constitutional rights of citizens and businesses. Such use would substantially increase the actual capacity of state security agencies to fulfill their mandates, proving to a great extent that privacy and security are not a zero-sum-game. On the contrary, there are combined technical and legislative solutions whereby one can strongly enhance the other.

2.10.3 Military and Defense

TC-compliant client devices is aimed at radically mitigating an increasingly crucial pain point of Germany - and its Armed Forces, as all other EU member states - in a new era of hybrid and asymmetric warfare, nearly impossible attribution of cyber incidents/attacks, rampant subversion deep down in the supply chain of high assurance systems, make the defense of the integrity and confidentiality of communications the key factor in achieving informational advantage.

Main use cases for initial deployment of TC-compliant client devices:

A. **Dual-use highly-confidential communications**. User is a mid or high public official, military officials, enterprise executive, public figure, or high-profile party member, willing to engage in lawful confidential personal or professional communications or negotiations with level so confidentiality and integrity assurance that are high or ultra-high.

B. **Military intelligence communications in urban environments**. User is a military intelligence operative with the need engage in sensitive remote digital communications while in busy public spaces. User may want to disguise the unit as a plain smartphone, and/or interface the device to tactical on-field radio communication unit;

C. **Military vulnerabilities reporting**. User may be a military official in active military operation needing to communicate to high military command about failures, vulnerabilities or diminished capabilities of an important military asset, physical, cyber or cyber-physical system.

TC-compliant client devices could amount to very thin standalone barebone handheld device, to seamlessly deliver radically unprecedented levels of confidentiality and integrity to the most critical strategic communication of high sensitive persons in high mobile, everyday scenarios, while solidly enabling legitimate and constitutional lawful access. They'd be conceived for future compliance with existing high-assurance IT certifications in mind, including NATO SECRET and EU SECRET though meant to substantially or radically exceed them.

In a second phase, TCCB - and compliant computing bases - would be applied to a wide variety highest-assurance communications, cloud and IoT domains that – in addition or alternative to confidentiality, integrity, authenticity and non-repudiability - require the **highest levels of availability and resiliency**, albeit compatible with the form factor, performance and power consumption characteristics of the computing base emerged from the 1st phase.

2.10.4 Algorithmic transparency and security of leading social media

The huge concentration of power in the formation of public opinion is accruing in those actors that own, most invest in, best utilize, best hack or "game" a few leading social media platforms, like Facebook/Instagram/Whatsapp and Twitter. After recent Russian influence on US elections, filter bubbles, "fake news" issues and Cambridge Analytica scandal, many have suggested more regulation.

While many have rightfully called for much more stringent antitrust measures and more user choice, many have also called for radically more **algorithmic transparency** in regards to critical algorithms that regulate discussion, post censoring, filtering, feeds generation security.

Such transparency however would be useless in restoring democracy and freedom unless (1) core algorithmic and systems complexity is mandatorily limited, to enable effective public assessment and (2) the core low-level root-of-trust systems are certified to levels of security. These are needed to achieve reasonable protection against large-scale undetected hacking or "gaming" of such algorithms, and therefore **algorithmic security and accountability,**

2.10.5 Artificial Intelligence and the Future of Humanity

It is becoming increasingly clear that the balance of power in society, and the prospects of well being for the human race, are and will be increasingly dominated by the emerging dynamics of formal and surreptitious control over the most advanced artificial intelligence systems and projects.

Rapid developments in AI specific components and applications, theoretical research advances, high-profile acquisitions from hegemonic global IT giants, and heartfelt declarations about the dangers of future AI advances from leading global scientists and entrepreneurs, have brought AI to the fore as both (a) the key to private and public economic dominance in IT, and other sectors, in the short-to-medium term, as well as (b) the leading long-term existential risk (and opportunity) for humanity, due to the likely-inevitable "**machine-intelligence explosion", or singularity,** once an AI project will reach or approach human-level general intelligence, at least in its capacity to improve itself.

A recent survey of AI experts estimates that there is a 50% chance of achieving human-level general intelligence by 2040-2050, while not excluding significant possibilities that it could be reached sooner. Such estimates may even be biased towards later dates because, (a) there is an intrinsic interest in those that are by far the largest investors in AI – global IT giants and US government – to avoid risking a major public opinion backlash on AI that could curtail their grand solo plans; (b) it is highly plausible, or even probable, that **substantial advancements in AI capabilities and programs may have already happened in civilian and military domains but have successfully kept hidden** for many years and decades, even while involving large numbers of people; as it has happened for surveillance programs and technologies of NSA and Five Eyes countries.

Stephen Hawking summarised the core challenges most clearly when he said, "***Whereas the short-term impact of AI depends on who controls it, the long-term impact depends on whether it can be controlled at all***".

Control relies on IT trustworthiness to ensure that those who control AI formally coincides with those who does so in practice, through hacking. It is unclear at this stage if *formal* control, in both the short- or the long-term, will have more influence on the nature of such AI systems than the *informal* control, i.e. the control exercised by those that have and will have sustained and undetected access to the most critical vulnerabilities of such systems.

In order to substantially reduce these enormous pressures, it is crucial to find ways by which sufficiently-extreme level of AI systems user-trustworthiness can be achieved, while at the same time transparently enabling due legal process cyber-investigation and crime prevention. Cyber-investigation capability may be crucial to investigate some criminal activities aimed at jeopardizing AI safety efforts**.**

Our solution to such dichotomy would reduce the level of pressure by states to subvert secure high-trustworthiness IT systems in general, and possibly – through mandatory or voluntary standards international lawful access standards – improve the ability of humanity to conduct cyber-investigations on the most advanced private and public AI R&D programs.

The Certification Body and its Paradigms, can become a crucial and fundamental element to increase the trustworthiness of the advanced narrow artificial intelligence systems (robots, self-driving cars, drones), and upcoming general artificial intelligence systems, by **increasing the trustworthiness of their most critical *deterministic* endpoints and sub-systems by orders of magnitude**. The dire short-term societal need and market demand for radically more trustworthy IT systems for citizens' privacy and security, and societal critical assets protection, can align – in a grand international vision – with the medium-term market demand and opportunity for large-scale ecosystems capable of producing AI systems that will be high-performing, low-cost and still provide adequately-extreme levels of security for AI critical scenarios.

Some may argue why extreme IT security to support AI safety is needed now if its consequences may be far away. One clear and imminent danger is posed by self-driving and autonomous vehicles (aerial and terrestrial) – which utilize increasingly wider narrow AI systems – and the ease with which they can be "weaponized" at scale. Hijacking the control of a large number of drones or vehicles could potentially cause hundreds of death or more, or cause hardly attributable hacks that can cause grave unjustified military confrontations.

Ideally, in our view, an international IT and AI trustworthiness standard setting and certification body governance - with extreme technical proficiency and citizen accountability, as per our proposed body - would exercise effective formal and informal control on all known large private and public advanced projects to ensure both safety and humanity values alignment or, better even, guide extremely well-founded international democratic nations' projects to develop "friendly AI", before "unfriendly AI" projects reach human-level general intelligence.

3 A Manifesto for Trustless Computing

Manifesto for a Trustless Computing Certification Body

The **world is rapidly turning into a Hacker Republic.** On one hand, most political and economic power accrues to those with sustained **informational and *malicious* hacking superiority** in critical communications and AI systems, resulting in a huge asymmetry of power between them and all others, creating two sets of citizens. On the other hand, ***ethical* hackers and whistleblowers** serve crucial public service to reign in such power by informing citizens and legislators, through revelations about critical vulnerabilities, unconstitutional state surveillance programs, and unearthing mass-scale crimes and frauds of the rich and powerful.

We believe that meaningful personal freedom and effective public safety in cyberspace may be **not "either or" choice, but a "both or neither" challenge** that can be radically improved through the **same kind of uncompromisingly distrustful oversight and certification processes** that produced unimagined levels of success in the safety of commercial aviation, the integrity of paper democratic election systems, and security of socio-technical systems for defense of weapons of mass destruction.

Neither freedom nor safety are available today because **all or nearly all communications IT systems are scalably compromisable** - even the most secure ones and cyber-investigation tools - by many **critical vulnerabilities and backdoors** that a few powerful nations have directly implanted or implicitly sanctioned by hugely financing the zero day market, by deliberate strategic subversion of key IT lifecycles, by not disclosing found vulnerabilities, and by deliberately promoting broken certification standards.

This state of affairs is inevitable for nearly all current systems, even high trustworthiness ones, because their technical and lifecycle complexity is by at least one order of magnitude beyond any sufficient verifiability, no matter what budget. It is not inevitable, on the other hand, for IT systems, services and lifecycle that would certifiably implement **extreme levels of transparency, accountability, oversight and ethical security-review relative to complexity** for all technologies and processes critically involved; from CPU design to fabrication oversight, from hosting facilities access management to standard setting governance.

Extreme compartmentalization, and minimization of features and complexity, in hardware and software, can economically allow radically-unprecedented and **consistently-extreme levels of ethical security review relative to the complexity of all software, firmware, hardware and processes** - including hardware design and fabrication, and hosting room management processes - that are critically involved in a TC-compliant IT service, and its lifecycle. The availability of at least one open low-level TC-compliant computing base will instead ensure wide uptake.

Meaningful digital confidentiality and integrity, ultimately, are not a product, nor a service or a process, but the by-product of the relevant organizational and human process that are critically-involved in fruition, provisioning and lifecycle of a given IT service or experience. It is therefore critical that "so called" *privacy-by-design* and *security-by-design* paradigms be brought to their ultimate conclusion, by requiring that IT services be trust-free, i.e. **devoid of the need or assumption of any unverified trust** in anyone or anything, except in quality of self-guaranteeing transparent and accountable organizational processes, that underlie all critical service and technology lifecycle and provisioning, whose quality is recognizable by moderately informed and educated citizens.

To a very large extent, the **extremely trustless technical, cyber-social and organizational safeguards** needed to ensure such ultra-high levels of user trustworthiness, are the **same** that can enable to offer voluntary lawful access compliance schemes - to such ultra-high trustworthiness IT services - that overall reduce the risks of abuse to the civil rights of citizens - and to the integrity and effectiveness of their cyber-investigation - to levels that are substantially lower than any other available secure IT solution.

The trustworthiness of an IT service should not be assessed according to compliance of part of its critical components to insufficiently comprehensive, state-subverted and self-referential certification standards, or according to reputation - as it is done today through the dominant "trusted computing model". Rather it will be measured through a utterly trustless fine-grained continuous modeling and real-time transparent monitoring of all relevant technological and procedural intrinsic constraints and all relevant organizational, economic, liability, legal and social behavioral disincentives, that might cause individuals and organizations critically-involved to perform unexpected compromising actions.

4 Acknowledgements

Authors:

Rufo Guerreschi, Executive Director at Trustless Computing Association and CEO at TRUSTLESS.AI. Has been leading bleeding-edge IT security R&D and certification initiatives, aggregating globally rare high-assurance open IT partners. CEO of TRUSTLESS.AI. Created the Free and Safe in Cyberspace events series. Brought the valuation of EU's 2nd largest tech/IT park from €3M to €21M. Previously, he led EU sales of J2ME provisioning, including the 10M€+ sale to Telefonica, then acquired by Motorola.

Udit Dhawan. (Phd) Co-lead Scientist at Trustless Computing Association and Endpoint Security Lead Advisor at TRUSTLESS.AI. Previously Technical Lead at Samsung Research & Development Institute, Senior Scientist at Intel Labs, Lead Student Architect on the US DARPA CRASH/SAFE project at University of Pennsylvania aimed at a clean-slate co-design of the entire computing stack for secure computation (now being commercialized by Dover Microsystems USA).

Special Contributor:

Roberto Gallo. (Phd) Co-lead Scientist at Trustless Computing Association, and Security Architecture Lead at TRUSTLESS.AI. Designed the World's 1st secure CPU that is inspectable in HW & SW source designs, in deployment since 2014. Designed security architecture of the 400,000 Brazilian voting machines & the ASI-HSM of the Brazilian PKI-root CA. Founded and lead Kryptus, a 50-people end-2-end hardware cybersecurity provider in Brazil.

Contributors:

This paper greatly benefited from hundreds of hours of discussions, suggestions and criticisms over 3 years with partners and advisors of the *Trustless Computing Association,* speakers of the *Free and Safe in Cyberspace[57]* event series and others. In particular by: Reinhard Posch (Austria CIO), Bart Preneel (Ku Leuven), Richard Stallman (FSF), Jovan Golic (Telecom Italia), Stefan Schuster (Tecnalia), Yvo Desmedt (U.Texas), Melle van den Berg (Capgemini Consulting), Peter Ide Kostic (EU Parliament LIBE Committee Secretariat), Michael Sieber (former EDA Head of Information Superiority), Christian Grothoff (GNUnet), Sven Herpig (Transatlantic Cyber Forum), Carlo Von Lynx (Secushare.org), Andrzej Białas (IbeMag), John Shamah (EEMA), Nicola Feltrin (U. Trento). James Fishkin (Stanford U.), Sunil Abraham (CIS India), Todd Davies (Stanford U.).

Inspirations:

We learned enormously and took much inspiration from the writings by Steven Bellovin, Bruce Schneier, Susan Landau; though some of their work made it so much harder for us to make our case.

5 References

1. Mills C. New Spectre-like flaws found in “virtually all” AMD processors. In: BGR [Internet]. 13 Mar 2018 [cited 11 Apr 2018]. Available: http://bgr.com/2018/03/13/amd-ryzen-spectre-ryzenfall/

2. Waqas. Teen Hacks Ledger Hardware Cryptocurrency Wallet. In: HackRead [Internet]. 22 Mar 2018 [cited 11 Apr 2018]. Available: https://www.hackread.com/teen-hacks-ledger-hardware-cryptocurrency-wallet/

3. Barrett B, Barrett B, Barrett B, Lapowsky I, Greenberg A, Matsakis L, et al. The Encryption Debate Should End Right Now. Wired. WIRED; 30 Jun 2017. Available: https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/. Accessed 11 Apr 2018.

4. Khandelwal S. Hacking Team sold Spyware to 21 Countries; Targeting Journalists and Human Right Activists. In: The Hacker News [Internet]. 24 Feb 2014 [cited 11 Apr 2018]. Available: https://thehackernews.com/2014/02/hacking-team-sold-spyware-to-21.html

5. Cox J. Someone Is Trying to Extort iPhone Crackers GrayShift With Leaked Code. In: Motherboard [Internet]. 24 Apr 2018 [cited 30 Apr 2018]. Available: https://motherboard.vice.com/en_us/article/qvx9jx/iphone-crackers-grayshift-graykey-leaked-code-extortion

6. Burrough B. How a Grad Student Found Spyware That Could Control Anybody’s iPhone from Anywhere in the World. In: The Hive [Internet]. Vanity Fair; 28 Nov 2016 [cited 22 Apr 2018]. Available: https://www.vanityfair.com/news/2016/11/how-bill-marczak-spyware-can-control-the-iphone

7. Cyberattacks prompt massive security spending surge [Internet]. [cited 11 Apr 2018]. Available: https://phys.org/news/2017-05-cyberattacks-prompt-massive-surge.html

8. Dave L. Forbes Welcome. Forbes com. 2016;

9. Vincent J. Putin says the nation that leads in AI “will be the ruler of the world.” In: The Verge [Internet]. The Verge; 4 Sep 2017 [cited 11 Apr 2018]. Available: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world

10. Use Tor or “extremist” Tails Linux? Congrats, you’re on an NSA list [Internet]. [cited 11 Apr 2018]. Available: https://www.theregister.co.uk/2014/07/03/nsa_xkeyscore_stasi_scandal/

11. Gallagher R, Greenwald G. How the NSA Plans to Infect “Millions” of Computers with Malware. In: The Intercept [Internet]. 12 Mar 2014 [cited 11 Apr 2018]. Available: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

12. Youtube. Jacob Appelbaum - People Think They’re Exempt From NSA (2014). Youtube; 2014.

13. Free and Safe in Cyberspace - event series. Michael Sieber @ Free and Safe in Cyberspace 2015 - EU Edition. Youtube; 2015.

14. Singh K. Trustless Computing Association. In: Trustless Computing Association [Internet].

Trustless Computing Association; 5 Mar 2018 [cited 22 Apr 2018]. Available: https://www.trustlesscomputing.org/

15. NSA Backdoors in Crypto AG Ciphering Machines - Schneier on Security [Internet]. [cited 11 Apr 2018]. Available: https://www.schneier.com/blog/archives/2008/01/nsa_backdoors_i.html

16. Dirtier than Watergate [Internet]. [cited 11 Apr 2018]. Available: https://www.newstatesman.com/blogs/the-staggers/2011/04/promis-government-inslaw

17. Martin J, Rappeport A. Debbie Wasserman Schultz to Resign D.N.C. Post. The New York Times. 24 Jul 2016. Available: https://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html. Accessed 11 Apr 2018.

18. Anderson R. Privacy versus government surveillance: where network effects meet public choice. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.656.6429

19. Villasenor J. If Apple Can Create A Backdoor To The iPhone, Could Someone Else? Forbes Magazine. 17 Feb 2016. Available: https://www.forbes.com/sites/johnvillasenor/2016/02/17/if-apple-can-create-a-backdoor-to-the-iphone-could-someone-else/. Accessed 15 Apr 2018.

20. Villas-Boas A. Some Android phone makers are reportedly lying about the security updates on their smartphones. Business Insider. BI; 12 Apr 2018. Available: http://www.businessinsider.com/android-phone-makers-caught-lying-about-security-updates-report-2018-4. Accessed 15 Apr 2018.

21. Hackett R. Apple Mac Updates Are Quietly Failing and No One Knows Why. In: Fortune [Internet]. [cited 15 Apr 2018]. Available: http://fortune.com/2017/09/29/apple-mac-update-security-sierra-firmware/

22. Guerreschi R. Cyber-libertarianism vs. Rousseau's Social Contract in cyberspace. In: Trustless Computing Association [Internet]. Trustless Computing Association; 24 Nov 2014 [cited 11 Apr 2018]. Available: https://www.trustlesscomputing.org/2014/11/24/cyber-libertarianism-vs-rousseaus-social-contract-in-cyberspace/

23. YouTube [Internet]. [cited 11 Apr 2018]. Available: https://youtu.be/FAskMLNwRPY?t=22m48s

24. How To Keep Your Wallet Recovery Seed Safe & Cryptocurrency Secure. In: Blockonomi [Internet]. 30 Oct 2017 [cited 11 Apr 2018]. Available: https://blockonomi.com/keep-recovery-seed-safe/

25. Holt A. A Troubling Analysis of the Recent Pew Poll on ISIS. In: Andrew Holt, Ph.D. [Internet]. 18 Nov 2015 [cited 11 Apr 2018]. Available: https://apholt.com/2015/11/18/65-649287-people-in-only-ten-majority-muslim-countries-support-isis-an-analysis-of-the-recent-pew-poll/

26. (www.dw.com) DW. Germany: Far-right violence and Islamist threat on the rise | Germany| News and in-depth reporting from Berlin and beyond | DW | 04.07.2017. In: DW.COM [Internet]. Deutsche Welle (www.dw.com); [cited 11 Apr 2018]. Available: http://www.dw.com/en/germany-far-right-violence-and-islamist-threat-on-the-rise/a-39534868

27. Press TA. Attorney-Client Privilege Is Not “Dead” _ and Not Absolute. The New York Times. Available: https://www.nytimes.com/aponline/2018/04/10/us/politics/ap-us-trump-russia-probe-attorney-client-privilege.html. Accessed 15 Apr 2018.

28. Economist T. Brazil’s Lula and government by judges. In: The Economist [Internet]. The Economist; 2018 [cited 22 Apr 2018]. Available: https://www.economist.com/news/americas/21740050-flaws-and-benefits-latin-americas-anti-corruption-drive-brazils-lula-and-government

29. Arlosoroff M. Four Israeli prime ministers, 20 years of corruption. Why? In: haaretz.com [Internet]. 28 Feb 2018 [cited 22 Apr 2018]. Available: https://www.haaretz.com/israel-news/business/.premium-four-prime-ministers-20-years-of-corruption-why-1.5850409

30. Gross G. Schneier on NSA’s encryption defeating efforts: Trust no one. In: PC World [Internet]. 16 Apr 2018 [cited 15 Apr 2018]. Available: https://www.pcworld.idg.com.au/article/525796/schneier_nsa_encryption_defeating_efforts_trust_no_one/

31. Schneier B. The risks of key recovery, key escrow, and trusted third party encryption. 1998.

32. Abelson H, Anderson R, Bellovin SM, Benaloh J, Blaze M, Diffie W, et al. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. 2015; Available: https://dspace.mit.edu/handle/1721.1/97690?show=full?show=full

33. Digital Transformation: Using Innovation to Combat the Cyber Threat. In: Federal Bureau of Investigation [Internet]. 7 Mar 2018 [cited 11 Apr 2018]. Available: https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat

34. YouTube L. YouTube https://youtu.be/uUXV2YPLtFc. Retrieved. 2011;27: 2011. Available: https://youtu.be/uUXV2YPLtFc

35. freesafe. Berlin, May 4th 2018 - Free and Safe in Cyberspace. In: Free and Safe in Cyberspace [Internet]. Free and Safe in Cyberspace; 15 Mar 2016 [cited 11 Apr 2018]. Available: https://www.free-and-safe.org/eu-edition-2018-berlin/

36. Greenberg A, Greenberg A, Newman LH, Barrett B, Bousquet CR, Greenberg A, et al. Researchers Point to an AMD Backdoor—And Face Their Own Backlash. Wired. WIRED; 13 Mar 2018. Available: https://www.wired.com/story/amd-backdoor-cts-labs-backlash/. Accessed 22 Apr 2018.

37. Germany, France lobby hard for terror-busting encryption backdoors – Europe seems to agree [Internet]. [cited 22 Apr 2018]. Available: https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/

38. Digital Transformation: Using Innovation to Combat the Cyber Threat. In: Federal Bureau of Investigation [Internet]. 7 Mar 2018 [cited 22 Apr 2018]. Available: https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat

39. Savage C. Justice Dept. Revives Push to Mandate a Way to Unlock Phones. The New York Times. 24 Mar 2018. Available:

https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html. Accessed 22 Apr 2018.

40. Local T. German government wants “backdoor” access to every digital device: report. In: The Local [Internet]. 1 Dec 2017 [cited 22 Apr 2018]. Available: https://www.thelocal.de/20171201/german-government-wants-backdoor-access-to-every-digital-device-report

41. Villasenor J. Compromised By Design? Securing the Defense Electronics Supply Chain. In: Brookings [Internet]. Brookings; 4 Nov 2013 [cited 15 Apr 2018]. Available: http://www.brookings.edu/research/papers/2013/11/4-securing-electronics-supply-chain-against-intentionally-compromised-hardware-villasenor

42. Rawnsley A, Rawnsley A, Newman LH, Barrett B, Bousquet CR, Greenberg A, et al. Fishy Chips: Spies Want to Hack-Proof Circuits. Wired. WIRED; 24 Jun 2011. Available: https://www.wired.com/2011/06/chips-oy-spies-want-to-hack-proof-circuits/. Accessed 22 Apr 2018.

43. Internet Society Chapters Webcasting. Snowden, the NSA, and Free Software - Bruce Schneier + Eben Moglen. Youtube; 2013.

44. Greenberg A. NSA Implementing “Two-Person” Rule To Stop The Next Edward Snowden. Forbes Magazine. 18 Jun 2013. Available: https://www.forbes.com/sites/andygreenberg/2013/06/18/nsa-director-says-agency-implementing-two-person-rule-to-stop-the-next-edward-snowden/. Accessed 28 Apr 2018.

45. Germanwings crash updates: Copilot had health, psychological problems, reports say. Los Angeles Times. 28 Mar 2015. Available: http://www.latimes.com/nation/la-fg-europe-germanwings-plane-crash-updates-20150326-htmlstory.html. Accessed 28 Apr 2018.

46. Serpro declara que não existe backdoor no Expresso [Internet]. [cited 15 Apr 2018]. Available: http://www.serpro.gov.br/menu/noticias/noticias-antigas/serpro-declara-que-nao-existe-backdoor-no-expresso

47. E-mail do Governo ganha mais uma proteção com solução nacional | CRYPTOID. In: CRYPTOID [Internet]. 6 Apr 2015 [cited 15 Apr 2018]. Available: https://cryptoid.com.br/arquivo-cryptoid/e-mail-do-governo-ganha-mais-uma-protecao-com-solucao-nacional/

48. barbara.wimmer. Gemalto-Hack: “Österreichische Reisepässe sind sicher” [Internet]. [cited 15 Apr 2018]. Available: http://futurezone.at/digital-life/gemalto-hack-oesterreichische-reisepaesse-sind-sicher/116.440.101

49. on High Performance Microchip Supply USDSBTF. Defense science board task force on high performance microchip supply. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; 2005.

50. Bellovin SM, Blaze M, Clark S, Landau S. Going Bright: Wiretapping without Weakening Communications Infrastructure. IEEE Secur Priv. IEEE Computer Society; 2013; 62–72. doi:10.1109/MSP.2012.138

51. Bellovin SM, Blaze M, Clark S, Landau S. Lawful Hacking: Using Existing Vulnerabilities for

Wiretapping on the Internet. 2013; doi:10.2139/ssrn.2312107

52. Government Hacking: Computer Security vs. Investigative Powers | Stiftung Neue Verantwortung (SNV) [Internet]. [cited 22 Apr 2018]. Available: https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

53. e.V C-SD. Angesichts professioneller Cyber-Angriffe auf Netzwerke der Bundesregierung – Cyber-Sicherheitsrat Deutschland e.V. fordert rasche und entschlossene Umsetzung der im Koalitionsvertrag festgehaltenen Vorhaben zu Cyber-Sicherheit - Cyber-Sicherheitsrat Deutschland e.V. In: Cyber-Sicherheitsrat Deutschland e.V. [Internet]. 12 Mar 2018 [cited 23 Apr 2018]. Available: http://www.cybersicherheitsrat.de/angesichts-professioneller-cyber-angriffe-auf-netzwerke-der-bundesregierung-cyber-sicherheitsrat-deutschland-e-v-fordert-rasche-und-entschlossene-umsetzung-der-im-koalitionsvertrag-festgeha/

54. Heumann S, Scott B. Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany1. Impulse . 2013;25: 2. Available: https://netzpolitik.org/wp-upload/Nr.25_Law_and_Policy_in_Internet_Surveillance_Programs.pdf

55. Rothman J. Takes: The N.S.A.'s Surveillance Programs. The New Yorker. The New Yorker; 6 Jun 2013. Available: https://www.newyorker.com/books/double-take/takes-the-n-s-a-s-surveillance-programs. Accessed 15 Apr 2018.

56. Lessig L. It's Time to Rewrite the Internet to Give Us Better Privacy, and Security. In: The Daily Beast [Internet]. The Daily Beast; 12 Jun 2013 [cited 15 Apr 2018]. Available: http://www.thedailybeast.com/articles/2013/06/12/it-s-time-to-rewrite-the-internet-to-give-us-better-privacy-and-security.html

57. freesafe. Speakers - Free and Safe in Cyberspace. In: Free and Safe in Cyberspace [Internet]. Free and Safe in Cyberspace; 24 Jan 2015 [cited 13 Apr 2018]. Available: https://www.free-and-safe.org/speakers/