Title: Psychological Harm: What is it and how does it apply to consumer products with internet connectivity?

Magda Osman[1,2]

1. Judge Business School, University of Cambridge, Trumpington St, Cambridge CB2 1AG.
2. Centre for Decision Research, Leeds Business School, University of Leeds, Leeds, West Yorkshire, LS2 9JT, UK.

Correspondence: m.osman@jbs.cam.ac.uk

Abstract

Consumer products with internet connection (hereafter CPIC) introduce a range of efficiencies into our day-to-day household activities. In combination, the network of CPIC in our home “smart homes” enable us to monitor and control devices remotely via our mobile phone. As with any technological innovation, with new benefits come concerns of new harms. Psychological harm is one such type. It is increasingly associated with CPIC, but to date there is no systematic analysis of the concept, and so this rapid review is a way of addressing this by organising relevant literature into three sections. Psychological and clinical research is most familiar with the concept, and this is where the review begins. By exploring how it characterised and measured there, it sets the groundwork for examining how the same concept is emerging in association with CPIC. This section starts with an in depth look at hazards (e.g. security breaches) to consider typical harms that present and then to understand where psychological harms could also occur. Thus far the findings suggest that psychological harms are not foremost of consideration in the mind of the consumer, criminal activities and privacy are the most prominent. The final section integrates the insights from the earlier sections to outline the inherent issues that need to be surmounted if the concept of psychological harm is going to be practically applied to the domain of CPIC.

Keyworks: Psychological Harm, Psychological Distress, Smart Products, Smart Home, Connected Devices

Section 1: Psychological harm as understood in the psychological sciences

While we can all appreciate what psychological harm refers to in a prosaic sense, there is a long history concerning what it has been taken to mean in technical applications of it for practical purposes such as in clinical assessments. Therefore, the aim here is to comprehensively review what the concept is and how it has been empirically investigated and applied in the psychological sciences, before then extending the concept to the domain of connected products with internet connection (CPIC).

1.1. Early use of the term psychological harm

Unsurprisingly psychological harm as a concept is not new in psychological science. It has a long history[1] first emerging as a label that captured the destabilising effects that propaganda employed during warfare was designed to achieve (Linebarger, 1946). The ominous experiences of being conscripted into armed services, along with the traumatic experiences during warfare (e.g. witnessing death, injury, destruction) were also where the term was applied (Bychowski, 1944). It later found its uses to capture the social stigmatisation of name calling in developmental work (Smythe & Seidman, 1957). The earliest popular application of the term was in the domain of consumer research (Bayton, 1958). The term was used in reference to the outcomes of methods that target different motivational factors, such as appealing to the emotions and insecurities of customers. This strategy was referred to as invoking "*Ego-defensive needs—the* needs to protect the personality; to avoid physical and psychological harm; to avoid ridicule and "loss of face"; to prevent loss of prestige; to avoid or to obtain relief from anxiety." (Bayton, 1958, p. 283). At the time psychodynamics was one of the dominant guiding frameworks for psychological research, and the application of it, as motivational research was commonly exploited in advertising (Packard, 1957).

When it came to the scientific practice of psychology, psychological harm referred to the experiences of human participants in experiments (Schultz, 1969). In the development of ethics codes of practice for conducting research the avoidance of psychological harm was a central consideration (Schlenker & Forsyth, 1977). A researcher is expected to eliminate the "possibility of harmful aftereffects and avoids them, or removes them as soon as permitted by the design of the experiment" APA,1963). A part of any standard appraisal of ethical issues is the mitigation of such experiences. This is now the main stay of any submission of an ethics application proposal before conducting an experiment. Even with available guidelines, in the research ethics context considerable judgment is still exercised about what might be psychologically harmful when granting approval for psychology experiments. The gulf between perceived psychological harm, and tangle physical and behavioural analogues is a problem here and will be a recurring theme as we proceed throughout this section.

Unfortunately, to date psychological research practice has absconded from defining psychological harm (Gale, 2019). This is resolved by psychological associations describing the features of psychological harm in published codes of practice (e.g. American Psychological Association, British Psychological Society). For example, psychological harm can manifest as discomfort, emotional stress, emotional harm, mental stress, psychological distress, negative emotions that undermine wellbeing, as well as negative emotions that may be experienced directly with violation of privacy (Gale, 2019; Oates et al., 2021; Olsen, 2023; Schlenker & Forsyth, 1977).

Suffice it to say, since the earliest entry of the term in academic literature, psychological harm encapsulates several phenomena that range from discomfort to trauma. Consequently, from its origins to date, psychological science does not offer a single overarching definition of psychological harm, nor does it offer a standardised inventory or scale that can measure it. Instead, psychological harm is

[1] One of the earliest references to psychological harm was in reference to a conference on maternity and child welfare, "Children should be taught that pre-marital intimacy caused psychological harm and tended to lead to unhappy marriages, while restraint before marriage led to more respect and happiness after the wedding day". (Spilsbury et al., 1936).

context specific, and therefore to understand what it is depends on the domain in which it has been studied. Wherever there are going to be adverse chronic or acute adverse experiences that impact on human activity, inadvertent or deliberate, there will be corresponding adverse psychological experiences which fall under the term psychological harm. The subjective nature of psychological harm also means considerable individual differences in how it is perceived when corresponded to events in the world.

1.2. Current conceptions of psychological harm in clinical domains

The literature is too vast to comprehensively explore the application of the term in every clinical psychological domain. The aim here is to synthesise the work to give a general indication of how the term is applied (see Table 1). Two things to observe here are that many definitions rely on illustrations of what harmful experiences occur as a substitute for a definition. Otherwise, the definitions refer to other psychological and behavioural consequences of psychological harm in attempt of some operationalisation of the term.

Insert Table 1 about here

First of all, just as with codes of ethics for conducting psychological research, clinicians also have codes of ethics, and, by extension, a do no harm principle. Accordingly, there are also measures of psychological harm that patients are screened for as a consequence of adverse treatment from mental health practitioners (e.g., Jonsson et al., 2014; Lilienfeld, 2007). Outside of the clinical profession itself, typically clinical instruments that screen for psychological harm are employed for serious psychiatric or medical conditions. For instance, psychological harm is assessed when screening for prostate and lung cancers, osteoporosis, abdominal aortic aneurysm (AAA) and carotid artery stenosis (CAS) (e.g., DeFrank et al., 2015; Kirkøen et al., 2016). The clinical assessments used here are designed to detect “anxiety, distress and decrements in health-related quality of life” as indices of psychological harm (DeFrank et al., 2015, p 242). Outside of medical contexts, where people find themselves in vulnerable situations that can cause persistent severe adverse psychological there are measurement tools to assess psychological harm. For instance, adverse situations that children find themselves in often require assessment of psychological harm (e.g. bullying (Montes et al., 2022), childhood abuse (e.g., Goldenson & Josefowitz, 2021), child and adolescent trauma (e.g., Wethington et al., 2008)). By the same token, adverse situations that adults face in places of work also have accompany assessments of psychological harm (e.g. prisons inmates (e.g., Humber et al., 2015), slaughterhouse workers (e.g., Dillard, 2008; Slade & Alleyne, 2023), military personnel and other professional situation in extremis (Johnson et al., 2011)).

The cyber domain is becoming a dominating avenue for clinical research, and the adverse impacts that it can produce, and is obviously pertinent to the overall focus of this review and so will be used to expose many of the pervasive issues of psychological harm in clinical assessment tools. Connecting to a virtual or online domain in and of itself has been argued to increase adverse psychological effects beyond those typically experienced offline. However, the evidence base is still emerging. As yet, it is not clear that our ever-increasing experiences online lead to chronic adverse effects on our mental health and wellbeing (Huang, 2010; Lippke et al., 2021; Vuorre & Przybylski, 2023). The causal mechanisms are still being investigated to be able to isolate factors to confidently assert what causes adverse effects and by what magnitude.

Outside of the analysis of adverse outcomes resulting from internet use, specific harms associated with specific types of abuses provides a much more concrete basis to tract hazards to their corresponding harms. For instance, one of the most common areas of clinical assessment is cyber bullying (Lim & Lee, 2021). There are spillover effects, such that activities in the virtual world can have tangible consequences in the offline world. For some, the evidence suggests that there is little difference between cyberbullying and traditional manifestations of bullying, for which findings show

common adverse outcomes. Victims of bullying are reported to be more likely to engage in unsafe sexual activities, substance abuse, suicidal ideation, self-harming, as well as suicidal behaviour (John et al., 2018; Litwiller & Brausch, 2013). There are a number of measurement scales to identify psychological harm to be able to treat the effects of cyberbullying (Kessler et al., 2002; Lim & Lee, 2021, 2022); see Table 2 for examples of items used in these scales. These scales are used alongside other clinical instruments that measure depression and anxiety (e.g. Vilariño et al., 2022) and posttraumatic stress disorder (PTSD). The manifestation of harm expresses itself in many ways which also have corresponding measures to determine psychosis, addictive behaviours, eating disorders, self-esteem, sleep patterns, and self-harm (e.g., Islam et al., 2022; Montes et al., 2022).

Insert Table 2 about here

For instance, regarding self-harm, suicidal ideation (considering committing suicide) is corresponded with records of suicide attempts (any attempt and an attempt requiring medical treatment) and self-injury (e.g. ‘‘How many times did you hurt or injure yourself on purpose?” (For example, by cutting, burning, or bruising yourself on purpose) (Schneider et al., 2012). Therefore, another important issue to highlight here is that, while some measures of psychological harm are specific to mental factors (e.g. experiences of negative emotions, rumination, suicidal ideation), items included in other scales identify physiological and behaviour outcomes associated with these negative mental states.

The main issue exposed here is the enormous conceptual confusion in the application of the concept of psychological harm. It can be a generic term that encapsulates all adverse psychological and behavioural consequences experience from cyberbullying and cyberstalking. Psychological distress (see Table 2) is used interchangeably with psychological harm, and other times it is defined as distinct (see section 1.3). Either as separate, or the same, both psychological harm and psychological distress have corresponding scales of assessment that are not on their own enough. They accompanied with clinical instruments that measure anxiety, depression and post-traumatic stress disorder alongside behavioural and physiological outcomes. The former is problematic because psychological harm/psychological distress also get conflated with depression, anxiety and PTSD, where each of these psychiatric disorders have their own distinct aetiologies and methods of treatment. All of these issues are not simply the result of emerging work on adverse effects in the cyber domain, all the problems exposed here equally apply to other domains (workplace settings, schools, psychiatric wards, hospitals) that screen for psychological harm.

1.3. Psychological Distress

It is worth examining the ways in which psychological distress is understood as a concept separate from psychological harm not least because it has consequences for how psychological harm specifically (rather than distress) could be applied in the domain of CPIC. For instance, a well-regarded definition of psychological distress which is employed in clinical and nursing practices is “the unique discomforting, emotional state experienced by an individual in response to a specific stressor or demand that results in harm, either temporary or permanent, to the person” (Ridner, 2004, p 539). Ridner (2004) uses the definition to help outline psychological distress can be measured in nursing practice and research (See Table 3), and Massé (2000) provides an alternative that converges on many of the same characteristics.

The central problem with psychological distress that pervades psychological harm are what the exclusion and inclusion criteria are. When reporting on areas where psychological distress is experienced, often depression, anxiety and PTSD are referred to as examples of psychological distress. It doesn’t stop there, psychological distress can also be taken to mean “affective distress, bodily distress, emotional distress, interpersonal distress, moral distress, subjective distress, neurotic distress, psychogenic distress, psychosocial distress, somatic distress, symptom distress” (Carrozzino et al., 2023, Page 235).

Insert Table 3 about here

For instance, in Carrozzino et al.'s (2023) review, they classify eight categories of phenomena that have been empirically shown to correspond to psychological distress: a sense of demoralization, the experience of feeling broken or mental pain, a sense of anguish, symptoms of somatization and ADHD, manifestations of anger, self-perceived lack of control, and a tendency to self-criticism associated with feelings of inferiority (Carrozzino et al., 2023). The latest Symptom Checklist-90 (SCL90) is a 90-item questionnaire used to screen for psychological distress and is the most comprehensive instrument currently available (Bech & Timmerby, 2018; Carrozzino et al., 2016; Carrozzino et al., 2023).

In studies examining psychological distress we see several battle grounds. Scholars and practitioners are at pains to point out that psychological distress should not be confused with these psychiatric disorders (e.g., Philips, 2009). Even with Ridner's (2004) commonly cited definition, there is a failure to show precisely how it can be empirically distinguished from psychological harm. The scales used to quantify psychological distress have come under considerable scrutiny because of concerns over their validity and reliability. Recent efforts to address this show promise, but come with a crucial caveat. Psychological distress is entirely subjective and so the magnitude of the experience is determined by the way an individual perceives it (Carrozzino et al., 2023; Ridner, 2004). In concrete terms, if one where required to go for a cancer screening, this could result in psychological distress. The experience of distress can be anxiety, but with no objective corollary regarding barriers to screening or following recommendations, which would be manifest harms to the individual's medical status (e.g. Chad-Friedman et al., 2017).

Psychological Injury and Psychological damage

Forensic psychology is another common arm of the psychological sciences where the concept of psychological harm is used (McGorrery, 2020), though here it is often referred to psychological injury (Kock et al., 2005) or psychological damage (Bornstein & Schwartz, 2009). One function of the discipline is to investigate what the appropriate legal thresholds are for actionable negligent or related injuries that have a psychological component (e.g. PTSD) but also those that might have physiological, neurological and medical components (e.g. chronic pain, traumatic brain injury) (Young et al., 2020).

The standards for identifying psychological injury or damage are high given that the basis on which adverse mental experiences occur has legal implications. A common view of psychological injury is that it includes stress related emotional conditions that are brought about from real or imagined threats or injuries that may become the subject of personal injury litigation, workers compensation claims, criminal injury, compensation, disability claims, or human rights tribunals (Kock et al., 2005). Typical disorders that fall under psychological injury include PTSD, acute stress disorder (ASD), major depression, substance abuse disorders, along with other complex anxiety and or depressive reactions. As a legal requirement there needs to be a causal mechanism that is demonstrated through evidence to attribute liability to another party (Kock et al., 2005).

The same standards also apply to specific manifestations of injury such as psychological damage. Generally psychological damage is taken to refer to pain, which can be experience mentally as well as physically, along with mental suffering, emotional distress, mental anguish, loss of enjoyment of life, anxiety, humiliation, shock. These examples of psychological damage bear a close correspondence to psychological distress, and evidence of them in forensic psychology is used to demonstrate impairments of faculties that are compensable. (Bornstein & Schwartz, 2009). Otherwise, compensation claims and estimating the size of a monetary award in cases where pain and suffering come from determining the recovery from psychological damage (Wissler et al., 2017).

Also, the evidence of psychological injury and damage for the purposes of establishing a causal mechanism can either show that, a victim prior to the injurious act or actions, had not experienced PTSD, or in situations where PTSD was a pre-existing injury, it was exacerbated by the injurious act or actions. In fact, a common basis on which to assess psychological injury is to use clinical assessments of PTSD (Wygant & Lareau, 2015). Measures like this are necessary because while the psychological injury is in and of itself important, it is often the economic costs associated with it that can be used to determine punitive measures and compensation. One important factor is the difficulty in evidencing psychological injury especially for attaching liability to a third party. This is particularly salient because the injury may not always manifest at the time, or even shortly after an injurious act or actions take place, and so delayed adverse psychological impacts while expected need to still be demonstrated as directly the result of an injurious act (McGorrery, 2020).

Unfortunately, the issue of conceptual clarity has not escaped the domain of forensic psychological research on psychological injury and psychological damage. Moreover, there are continuing debates about the appropriate methods of assessment to reliably measure both, as well as the establishment of causality. Often evidence of adverse physiological, neurological, and medical outcomes accompanies evidence from clinical instruments to demonstrate the presence of psychological injury and damage. As was the case with psychological harm and psychological distress, here also the common clinical instruments (e.g. PTSD, Depression Inventories, Anxiety Scales) are used to demonstrate the presence of psychological injury and damage. They instruments are also used to detect those fraudulently seeking compensation or other punitive measures by feigning psychological injury and damage (e.g., Bush et al., 2014; Fokas & Brovko, 2020; Sáncheza et al., 2017; Vilariño et al., 2013).

1.4. Summary of Psychological harm in the psychological science

Before going on to discuss the emergence of psychological harm in consumer products with internet connection (CPIC) this summary section takes stock of the general insights that can be drawn from how the concept is understood in psychological science. It is clear that psychological harm is multifaceted. It manifests in different domains meaning there may well be unique profiles of adverse mechanisms that can cause it to be expressed in various ways. For instance, the injurious acts associated with cyberbullying are the not the same as cyberstalking, and while there might be a common pattern of adverse mental and physiological consequences, the profiles will differ. For this reason, it is understandable – and understood - that definitions of the term will be context specific. The inclusion and exclusions criteria for psychological harm are also hard to determine, not least because of the dependency on descriptions that veer into anxiety, depression and PTSD. Psychological harm when studied often relies on evidence beyond self-reports to demonstrate harms to the individual as physiological and behavioural. The clearest illustration of this is in legal contexts. In pursuit of punitive measures, the causal path between adverse injurious acts to adverse mental experiences is easiest to demonstrate when accompanied by evidence of objective observable manifestations (i.e. physiological and behavioural).

Section 2: Consumer products with internet connection (CPIC)

In the domain of consumer products, typically harms, especially those that are considered in risk assessments, focus on physical harms (e.g. choking from a small detachable part of a toy), environmental harms (e.g. toxic substances that leak into soil) and financial harms (e.g. cost of recovery from a consumer product related fire). Given that the range of functions of conventional consumer products have changed with the advent of technologies that connects them to the internet, it makes sense to consider what new hazards and harms might present.

CPIC are alternatively referred to as smart devices (e.g., Hickey et al., 2021; Silverio-Fernández et al., 2018; Sikder et al., 2021), smart homes (because many devices are connected within a network of devices in a home) (e.g., Alaa et al., 2017; Lutolf, 1992; Marikyan et al., 2019; Serrenho & Bertoldi,

2019; Solaimani et al., 2015; Sun & Li, 2021), or Internet of Things (IoT) connected devices (Abdul-Qawy et al., 2015; Lupton, 2020; Madakam et al., 2015; Olabode et al., 2023). There is a considerable range of consumer products that this general description applies to (e.g. large appliances, security cameras, baby monitors, pet feeders, alarm systems, toys), some of which are wearable (e.g. watches, health monitors, fitness devices, clothing), and with an ever-increasing expansion of functions associated with them (e.g. voice activated personal assistants such as Amazon Alexa, Google Home). While there are differences in how CPIC are construed, there are core family resemblances. They are physical objects that contain sensors along with software that connect them to other devices (e.g. smart phone, personal computer, laptop, tablet) and critically they all depend on a wireless sensor network.

Many of the aforementioned reviews concerning CPIC (e.g. smart devices, smart homes, IoTs) have considered at length the technological and safety issues that they present (e.g., Alaa et al., 2017; Abdul-Qawy et al., 2015; Hickey et al., 2021; Lupton, 2020; Madakam et al., 2015; Olabode et al., 2023; Serrenho & Bertoldi, 2019; Silverio-Fernández et al., 2018; Sikder et al., 2021; Solaimani et al., 2015; Sun & Li, 2021). In addition, several reviews have focused explicitly on the emerging range of common adverse consequences that CPIC present (Buil-Gil et al., 2023; Farhadloo, Asvadi, & Khorasani, 2024; Fu et al., 2020; Moh et al., 2023; Olabode et al., 2023).

The dominant issues that have been raised in association with CPIC are privacy, security and relatedly, vulnerability to cyberattacks (e.g. Buil-Gil et al., 2023; Chhetri & Motti, 2022; Gai et al., 2018; Meidan et al., 2020; Rutledge, Massey, & Antón, 2016). However, to date, none have explicitly referred to, or proposed the concept of psychological harm. Therefore, the starting point of this section is to review the common hazards and associated harms in the CPIC literature to then explore where psychological and social harms could apply.

2.1. CPIC: Common hazards

The capabilities that CPIC offer come from sensing nodes that track and transmit sense data that connect physical and cyber worlds through telecommunications (e.g. Orfanos et al., 2023). Thus, products with these capabilities offer users the opportunity to remotely monitor and control how products operate, or use settings to enable the products to perform automatically. Two problems are commonly highlighted, technical inherent issues to do with hardware, and software issues. For instance, there are inbuilt limitations regard energy efficiency of CPIC because they are powered by batteries that present restricted capacity that are difficult or even impossible to recharge or replace (e.g. Evangelakos et al., 2022; Nakas et al., 2021; Orfanos et al., 2023). Other inbuilt factors can impact the normal performance of CPIC such as limited data storage, limited computational power, loss of connectivity (e.g. Farsi et al., 2019; Keerthika & Shanmugapriya, 2021), and congestion. Congestion is when multiple sources of data attempt transmission at the same time through the same channel, and where the entry point fails to forward or receive the incoming data (e.g., Kandris et al., 2017). The consequence is CPIC deteriorates in functioning normally (e.g. Keerthika & Shanmugapriya, 2021; Sharma et al., 2021), this will be revisited in the context of Distributed Denial of Service (DDoS) attacks.

While these technical issues present challenges regarding the performance of the products, given the range of products that can be connected, and the range of sensory data that is transmitted, the latter can also generate technical challenges, and where vulnerabilities emerge. For instance, CPIC interconnected in a home (see Figure 1 as an illustration of this) means there needs to be standardized communication technologies that offer efficient ways for monitoring and control (e.g., Orfanos et al., 2023). Typically, users have monitoring and control access through their smart phones, personal computers, laptops or tablets. Alternatively, and for the purposes of enhancing efficiency, large tech companies (Apple (HomeKit) Google (Alexa), Samsung (SmartThings)) offer ways of solving the problem of providing a unifying system. These options enable multiple controls through their own

platforms, as well as CPIC that are directly compatible with their own systems (e.g. Apple HomeKit) (Orfanos et al., 2023) but as will later be discussed, this exposes many access points for security breaches.

Insert Figure 1 about here

Beyond the inherent technological issues that CPIC present (e.g. energy efficiency, cost and data quality) the main concern is security (Ali et al., 2017). Ali et al (2017) set out five basic security goals that CPIC should adhere to: Authentication, Authorisation, Confidentiality, Integration and Accessibility, with five corresponding types of security protections: 1) verification that the user(s) of the CPIC are the authorised users, 2) every user has access rights as defined for the purpose of the CPIC, 3) only authorized users can access the private data within a system, 4) the data is maintained in consistent and accurate way, along with notifications of any modification or loss of data, 5) for any authorized user, all services will always be available and these resources are protected against any type of threat.

Another way to think about security is to distinguish problems with security in terms of passive and active attacks (Ali et al., 2017; Saxena et al., 2020). In the former case access to and monitoring of data is carried out in ways that do not disrupt the function of CPIC or the data itself, this is surreptitious and so hard to detect. In the latter case an adversary uses data, typically gathered through a passive attack to directly influence or alter the operation of CPIC (Ali et al., 2017; Keerthika & Shanmugapriya, 2021). Examples of active attacks often fall under cybersecurity operations which we are familiar to us: malicious software, email phishing attack, message and data modification, man-in-the-middle, identity theft, device hijacking, spoofing and distributed denial of service (DDoS) (Ali et al., 2017; Aldahmani et al., 2023; Lee et al., 2014). The general motivations of active attacks are to change, destroy, intercept, manipulate, or steal data (Aldahmani et al., 2023), and for passive attacks the motivation is stalk and control.

The hazards (typically referred to as vulnerabilities in cybersecurity literature) that CPIC present, as well as hubs that consolidate controls across multiple CPIC can be thought of as the causes of harms to users (Aldahmani et al., 2023; Buil-Gil et al., 2023; Chhetri & Motti, 2022; Gai et al., 2018; Meidan et al., 2020; Rutledge, Massey, & Antón, 2016). The harms are most commonly associated with security breaches are access to data and privacy. Date of birth, name, home address, and credit card details are critical customer information that companies hold for most CPIC. This means that customers entrust companies with having the necessary protections in place so that this data is not subject to attack. Depending on the CPIC other sensitive data that is collected (e.g. medical information) presents further priorities to protect customers data. Accordingly, companies have legal (and moral) responsibilities concerning their own security operations in response to ransoms threatening to release consumer data (e.g., Aldahmani et al., 2023; Buil-Gil et al., 2023).

Outside of the necessary security services that companies are required to provide for data storage and handling, other hazards identified can be classed under six types: 1) outdated protocols, 2) weak encryption, 3) limited storage and CPU, 4) insecure applications, 5) poor authentication, and 6) firmware failure (e.g., Abdullah et al., 2019). Alternatively, Davis et al., (2020) groups the hazards into four key categories (physical, network, software, and encryption), and Aldahmani et al. (2023) into three (perception, network/traffic, applications). Sensors, physical objects (i.e. perceptual properties of CPIC), routers (i.e. network) and the applications installed on CPIC devices themselves (applications) each pose a vulnerability to a security attack with similar consequences. These can be physical damage to the CPIC, disrupting the function of all CPIC, control of the operations of CPIC, and breach of privacy. The routers (i.e. network) is the means of connecting multiple CPIC together and support monitoring and control function. Buil-Gil et al.'s (2023) review of 106 studies provides a

current break down of common consequences (harms) of security breaches: Privacy intrusions (72.1%), hacking (67.4%), malware (51.2%), DDoS (48.8%) and stalking (7.0%). The next section considers in depth the criminal activity that comes from the various ways in which security breaches can occur through the aforementioned vulnerabilities.

2.2. CPIC: Criminality and commonly associated harms

The focus here is to outline the various crimes that have been examined in the literature that in turn present harms to CPIC users that are manifest as sexual and physical, financial, property, and privacy.

First, access to personal information as data theft is common, with the purpose of selling it to underground marketplaces (e.g., Bugeja et al., 2017; Jacobsson et al., 2016; Somasundaram & Selvam, 2018). While not the same, there is a corresponding issue regarding service provider's sale of user data to third parties without authorisation (e.g., Heartfield et al., 2018; Tabassum et al., 2019).

In addition, access to credit card details along with other critical information present a harm to personal finances particularly through theft, identify theft (e.g., Aldahmani et al., 2023; Heartfield et al., 2018; Iten et al., 2021), and even electricity theft (e.g., Ali et al., 2017; Abraham et al., 2024; Li et al., 2019). Emerging concerns around intellectual property theft (e.g. Heartfield et al., 2018) are a result of increases in the workforce working from home. Security hazards that present in voice command devices or personal home assistants can be used to access critical company information that is shared with colleagues over video conferencing (e.g., Heartfield et al., 2018; Taplin, 2020).

Financial loss can come in many forms such as costs in replacement of stolen items, or replacing CPIC because they have been maliciously tampered with, and through property damage because maliciously tampered CPIC cause fire related incidents (e.g., Iten et al., 2021; Tanczer et al., 2018). Financial losses can be incurred as a result of property damage or vandalism (Panwar et al., 2019). For instance, access gained by exploiting security vulnerabilities can enable malicious actors to control voice commands to then disable home security systems (e.g. security alarms, door locks). Activities of this kind are combined with ways of tracking domestic activities in the home through usage of CPIC to then determine optimal times to physically breach homes (e.g., Buil-Gil et al., 2023; Heartfield et al., 2018; Olabode et al., 2023) or damage property. The same methods, as well as coordination with other types of data accessed by means of security hazards, expose users to invasion of privacy through stalking online and offline (e.g., Blythe & Johnson, 2021; Iten et al., 2021). By association, stalking, in domestic abuse cases, though not restricted to this, enables attackers to track their victims with the intent to do physical harm, carry out sexual assaults, or homicide (e.g., Blythe & Johnson, 2021; Slupska & Tanczer, 2021; Tzezana, 2016).

Security hazards such as hacking in turn expose vulnerable users such as children to harm (e.g., Blythe & Johnson, 2021; Hall et al., 2020). This can include stalking and voyeurism of children through toys and other CPIC that include cameras. In addition, attackers can directly communicate with children though CPIC that have voice commands and speakers. Along with stalking, security hazards give attackers the opportunity to conduct various criminal activities, that include grooming where contact through devices is exploited, or actively exposing children to damaging material that is either violent, sexual, or both (e.g., Blythe & Johnson, 2021; Buil-Gil et al., 2023; Hannan Bin Azhar et al., 2023; Heartfield et al., 2018; Tzezana, 2016).

Another documented crime is blackmail where malicious actors access sensitive information of CPIC users (e.g., Blythe & Johnson, 2021; Buil-Gil et al., 2023; Tzezana, 2016). Here related harms are reputation damage (e.g. through public shaming of compromising information), as well as physical harm where threats of a physical nature are made if demands are not met, otherwise there are also financial losses if blackmail demands are met, or legal action is taken (e.g., Heartfield et al., 2018). Furthermore, accessing as well as recording (Tzezana, 2016) of sensitive information can be used in other malicious where threats of exposure of information are designed to prevent or harm a user's

employment status, as well as their credit or insurance status (e.g., Blythe & Johnson, 2021; Buil-Gil et al., 2023).

2.3. CPIC: Edge cases of criminality and associated harms

Hazards concerning security of CPIC can result in harms concerning the normal functioning of CPIC. Given one of the motivations of attackers is to assert control, one way in which this can be done is the unauthorised switching on or off of lights, heating, ventilation, air conditioning and other settings that users hand inputted into CPIC (e.g. Aldahmani et al., 2023; Heartfield et al., 2018). The associated harm is a breach of privacy, as well as disruption to normal domestic activities, though as a consequence disruption to the function of CPIC can also lead to physical consequences such as fires (e.g. if CPIC are turned on and are unattended) and consequently financial losses (e.g. Aldahmani et al., 2023; Iten et al., 2021).

As mentioned, other forms of active attack involve DDoS which also are a means of disrupting or prohibiting the normal function of CPIC, and here also similar types of associated harms are documented (Blythe & Johnson, 2021; Buil-Gil et al., 2023; Goudarzi, et al, 2021; Iten et al., 2021; Tzezana, 2016). The most consequential outcome associated with DDoS attacks concerns safety critical monitoring functions of CPIC such as fire and smoke detectors and alarms, which in turn cause physical harms, property damage and financial loss. Though other non-safety-critical functions of CPIC, such as lightbulbs, can nonetheless be overloaded (i.e. congestion) through DDoS attacks, producing similar consequences if occupants of dwellings are not present to switch lights off (Blythe & Johnson, 2021; Heartfield et al., 2018; Trimananda et al., 2018).

Malicious actors are able to use security hazards as a means of inserting false information into CPIC, again as a way of disrupting the normal functioning of CPIC, or as a means of control where they can manipulate user's actions (Aldahmani et al., 2023; Blythe & Johnson, 2021; Heartfield et al., 2018). Other attempts to disrupt the normal function of CPIC involve battery draining attacks (e.g., Blythe & Johnson, 2021; Heartfield et al., 2018; Kuaban et al., 2023; Smith et al., 2021) that in turn can present financial losses. There are various ways by which the prevention of CPIC functioning can be achieved through battery drainage, such as denial of sleep through a constant jamming of signals (a form of congestion), or flooding attacks that create massive amount of traffic that exhaust CPIC, and vampire attacks which use complex feedback loops where data packets cycle round a network and are distorted which also has the effect of draining batteries or consuming considerable energy (Smith et al., 2021).

The general issues that concern all these types of harms is that the effort by attackers is to disrupt or prevent the normal functioning of CPIC, and to reducing the ability of users to carry out their normal domestic activities. However, in many of these cases, the consequences are more severe because there are ensuing safety issues, security issues, physical harm, property damage, as well as financial losses.

2.3. CPIC: Psychological harms

The survey work (both quantitative and qualitative) examined user's common concerns regarding CPIC in the home overwhelmingly reflect privacy concerns and loss of control (e.g., Adeyeye, 2024; Cannizzaro et al., 2020; Chan-Olmsted et al., 2024; Cobb et al., 2021; Haney & Furman, 2023; Jaspers & Pearson, 2022; Korneeva et al., 2021; Schomakers et al., 2021; Turner et al., 2022).

But what about user's psychological experiences? While limited, there is work that has started to explore this (e.g. Pal et al., 2021; Raff et al., 2024). Pal et al (2021) devised survey items to identifying what they referred to as psychological concerns: e.g. A smart-home is not a good fit with my lifestyle; A smart-home will not fit in with my self-image or self-concept; A smart-home will make me lose control of my home. In their findings, when responses were considered in relation to the main focus of the survey which was privacy issues, psychological concern was less salient than physical concerns, which included the following items: I am concerned that smart-home devices may

continuously monitor my activities; I am concerned that someone may break into my house by utilizing the smart-home devices; I am concerned that the smart-home devices can be misused by others regardless of my will; When using a smart-home, I am concerned that someone may peep into my private life. Raff et al (2024) focused on user experiences of CPIC such as voice assistants by measuring perceived "creepiness" (e.g. I feel insecure around this smart home assistant; This smart home assistant makes me feel uncomfortable) as predictor of resistance to adoption of use of the device.

Because the vast majority of surveys focus primarily on privacy, trust, and user experiences of CPIC, psychological harm is not reported on because it simply isn't measured. One way around this is to look to qualitative work because respondents have a greater opportunity to spontaneously volunteer their experiences of psychological harm. In their qualitative interviews with 17 individuals from 7 households Kennedy et al (2021) found that the dominating topic of concern was privacy and trust in organisations to address privacy concerns. Psychological distress was mentioned, though only once, and in connection to children's use of CPIC. Along with a quantitative survey, Turner et al (2022) also conducted interviews with 25 families, and found that parents, guardians and children discussed threats and risks of online safety (e.g. stranger danger, cyber bullying, scams). When specifically discussing CPIC the concerns were financial fraud – and unauthorised spending of money, hacking that resulted in burglaries, physical damage and privacy breaches, and strategies in place to avoid children breaking devices. Interviews have also been conducted with older adults and their caregivers (e.g., Choi et al., 2021; Dermody et al., 2024; Ghorayeb et al., 2021). The common issues that were raised were privacy, affordability of CPIC, battery life, and general usability issues (i.e. convenience of use), but also their benefits by improving safety and alleviating some burdens on carers. Overall, the indication from the qualitative work is that psychological harm is not the foremost concern voiced by those taking part in qualitative research on CPIC.

While sparce, studies are exploring broader adverse effects of breaches of security of CPIC such as loss of control, loss of personal agency, and social isolation (Apthorpe et al., 2022; Bernd et al., 2022; Iten et al., 2021; Lee & Lim, 2024; Olabode et al., 2023; Shalawadi et al., 2024; Tanczer et al., 2018). Social isolation is revealed through intergenerational tensions (e.g. digital natives and digital nomads) in the home over the dependency on CPIC (e.g., Apthorpe et al., 2022; Bernd et al., 2022; Lee & Lim, 2024; Shalawadi et al., 2024). Another interpersonal angle that has been exposed is bystander privacy. Those present in homes that are not owners (i.e. bystanders) of the devices (e.g. nannies, carers, friends, family, guests, tenants) may still be exposed to security breaches of CPIC by dint of being present in the home at the time (Albayaydh & Flechais, 2024; Apthorpe et al., 2022; Despres et al., 2024). Intrusion of privacy is strongly associated with perceptions of loss of control and agency by users of CPIC (Gøthesen et al., 2023; Hall et al., 2020; Heartfield et al., 2018; Olabode et al., 2023; Paupini et al., 2022; Tabassum et al., 2019; Zimmermann et al., 2019). For both loss of control and agency, intrusion of privacy is attached to security breaches but also service providers that have access to personal information (e.g. voice assistants).

In the absence of any dedicated research on psychological harm in association with CPIC, Agrafiotis et al's (2018) taxonomy of cyber harms may be a useful starting point. This is a comprehensive framework for identifying categories of harms, though this was designed for application in general to cyber domains, and not specifically to CPIC. The taxonomy has five superordinate categories: Physical, Economic, Psychological, Reputational, Social/Societal. Under the Psychological, there are a list of 12 terms: Confusion, Discomfort, Frustration, Worry/Anxiety, Feeling upset, Depressed, Embarrassed, Shameful, Guilty, Loss of self-confidence, Low satisfaction, Negative changes in perception. The overarching objective of the taxonomy is as a conceptual framework for researchers and policy makers that can be used to identify a variety of harms in order to measure their prevalence and developing strategies to mitigate them.

Section 3: Addressing psychological harm from CPIC

In the domain of CPIC, the most common hazard is security breaches. From security breaches, there are a host of criminal activities, and in turn there are several harms that present (e.g. physical injury, damage to the home, financial losses). We are at early stages in determining the frequency of security breaches of CPIC and in turn the likelihood and severity of the harms that ensue. Of the many harms that are associated with different types of criminal activity from security breaches it is inevitable there will be psychological impact on those experiencing them. Empirical investigations looking into user's concerns regarding CPIC overwhelming point to privacy and security. Even when presented with opportunities to refer to other experiences, psychological harm is absent. Instead, respondents refer to tangle outcomes (e.g. fraud, privacy breaches) that they see a need to be addressed. Therefore, one question worth answering in this concluding section is what might be the practical value to policy in developing metrics to assess psychological harm in the domain of CPIC?

Firstly, if policy and legislation is inadequate in addressing the many ways in which security breaches can occur, then the rate of breaches could increase. The consequence would be that the public are increasing exposed to more hazards, and more criminal acts. This in turn means more victims of crime and associated harms, each of which will impact those exposed to them psychologically.

Secondly the possibilities to innovate the functions of CPIC means that the sheer volume of CPIC will increase, and in turn increase the vulnerabilities to security breaches. Consequently, we can play out the same doomed scenario where the more innovative the CPICs the more vulnerabilities there are likely to be, and the more likely it is for them to be exploited in ways that will result in even greater harms (either by magnitude, severity, or both) to users.

Finally, the gloomiest scenario is a combination of the first and second that reflect a state of the world such that the exposure to security breaches and in turn, their harms, becomes so vast as to be insurmountable for policy and legislation to effectively mitigate. In all three situations described there might be a case for including metrics of psychological harm alongside statistics on the type of breaches and the types of criminal activity that are committed. While the remit for policy and regulation is to mitigate the hazards, and enforce legislation, generally understanding the detrimental psychological effects people experience is useful even if not in any way actionable.

Regarding the first scenario, Various market research organisations (e.g. STATA, Yougov) have been surveying populations to determine market share of CPIC. In terms of adoption, there is an estimated 14.2% of households worldwide that had CPIC that would constitute a smart home, and this is estimated to increase to 28.8% of households worldwide by 2027 (Stata, 2024). In the UK, approximately 39% of households own CPIC used in the home (e.g. smart speakers, thermostats, security systems); by 2027 this is estimated to increase to 50.2% (Ukpana, 2024). While it is hard to abstract from these estimates in changes to the magnitude and severity of harms users will be exposed to, it might be possible to extrapolate from the current evidence based (e.g. Buil-Gil et al., 2023).

In any case, because of these market trends many countries are increasing their regulatory and legislative powers to address the CPIC security and safety issues (e.g. the UK's Product Security and Telecommunications Infrastructure Act (PSTI Act) of 2022; the EU Cyber Resilience Act (CRA) 2024; the US Informing Consumers about Smart Devices Act, 2024; China's Regulations on the Management of Security Vulnerabilities in Network Products Law, 2021; Canada's Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, currently still in the process of being passed; United Nations (UN) 2023 working paper on 'The regulatory compliance of products with embedded artificial intelligence or other digital technologies'). How these regulatory and legislative powers take effect in mitigating security and safety issues will take time to evidence, not least because baseline data needs to be collected to assess efficacy. Given what has already been explored in empirical work discussed in this

review, one avenue worth exploring is the reduction in user's concerns over privacy and security as a consequence of the various measures enforced.

In addition to conventional metrics of physical, financial and property harms, for policy or regulation to make a case for using metrics of psychological harm would require empirically answering the following question. In the absence of criminal activity, or edge cases of criminal behaviour associated with CPIC, what types of psychological harms are experienced that would require a policy or legislative response? The question is posed in this way because what is critical here is identifying what needs to be mitigated. If psychological harm is inevitably mitigated because other harms (e.g. financial harm, property damage, physical harm) are mitigated through efforts to address known hazards, then why would there be a need to address psychological harm exclusively?

So far research on psychological harm from CPIC is too junior for any concrete answers to this question. We can instead look to a potential answer to this question comes from the work reviewed in areas of psychology (e.g. clinical psychology, forensic psychology). But we see several hurdles that need to be overcome. The first of which is that there is no standard definition of psychological harm or a standardised metric of psychological harm that could be applied to CPIC. Second, as was discussed in relation to forensic psychology and the examination of psychological injury and psychological damage, the standard for evidence is high because of the need to establish a causal mechanism. The field of forensic psychology has offered some practical ways for acquiring evidence to demonstrate a causal path from injurious actions to psychological injury. Given the standard of evidence, psychological injury or damage is accompanied by instruments that clinical professionals use to assess psychiatric disorders, along with accompanying physical, neurological, behavioural and medical outcomes. The same approach could be extended to CPIC would show how injurious acts experienced from CPIC cause psychological harm alongside, not independent of other measurable objective harms which would need to be mitigated (e.g. financial harm, property damage, physical harm).

If we are to take seriously what people are concerned with then there is plenty of evidence to show where attentions should be focused. As has been highlighted in this review, CPIC users are concerned with intrusion of privacy, trust in the service providers, and lacking the means to control their own data under normal functioning of CPIC, as well as when breaches occur. There is an important role research can play, especially researchers experienced in the domain of risk analysis, to explore the practical implications these concerns have for policy and regulation around CPIC.

References

Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur*, *19*(9), 139.

Abraham, O. A., Ochiai, H., Hossain, M. D., Taenaka, Y., & Kadobayashi, Y. (2024). Electricity Theft Detection for Smart Homes: Harnessing the Power of Machine Learning With Real and Synthetic Attacks. *IEEE Access*, *12*, 26023-26045.

Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The internet of things (iot): An overview. *International Journal of Engineering Research and Applications*, *5*(12), 71-82.

Adeyeye, K. (2024). Controlling the 'elephant in the room': A new protocol for sharing data from home performance monitoring systems. *Technology in Society*, *76*, 102478.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of network and computer applications*, *97*, 48-65.

Albayaydh, W., & Flechais, I. (2024). " Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1-54.

Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology*, *4*, 281-292.

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. In *2017 23rd International Conference on Automation and Computing (ICAC)* (pp. 1-6). IEEE.

Apthorpe, N., Emami-Naeini, P., Mathur, A., Chetty, M., & Feamster, N. (2022). You, me, and IoT: How internet-connected consumer devices affect interpersonal relationships. *ACM Transactions on Internet of Things*, *3*(4), 1-29.

Bayefsky, R. (2015). Psychological Harm and Constitutional Standing. *Brook. L. Rev.*, *81*, 1555.

Bayton, J. A. (1958). Motivation, cognition, learning—basic factors in consumer behavior. *Journal of Marketing*, *22*(3), 282-289.

Bech, P., & Timmerby, N. (2018). An overview of which health domains to consider and when to apply them in measurement-based care for depression and anxiety disorders. Nordic Journal of Psychiatry, 72(5), 367–373.

Bernd, J., Abu-Salma, R., Choy, J., & Frik, A. (2022). Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (pp. 687-706).

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, *34*, 97-125.

Bornstein, B. H., & Schwartz, S. L. (2009). Injured body, injured mind: Dealing with damages for psychological harm. *Jury Expert*, *21*, 33.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)* (pp. 557-562). IEEE.

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, *145*, 107770.

Bush, S. S., Heilbronner, R. L., & Ruff, R. M. (2014). Psychological assessment of symptom and performance validity, response bias, and malingering: Official position of the Association for Scientific Advancement in Psychological Injury and Law. *Psychological Injury and Law*, *7*, 197-205.

Bychowski, G. (1944). Personality changes characterizing the transition from civilian to military life. *The Journal of Nervous and Mental Disease*, *100*(3), 289-296.

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *Plos one*, *15*(5), e0231615.

Carrozzino, D., Patierno, C., Pignolo, C., & Christensen, K. S. (2023). The concept of psychological distress and its assessment: A clinimetric analysis of the SCL-90-R. *International Journal of Stress Management*, *30*(3), 235.

Carrozzino, D., Vassend, O., Bjørndal, F., Pignolo, C., Olsen, L. R., & Bech, P. (2016). A clinimetric analysis of the Hopkins Symptom Checklist (SCL-90-R) in general population studies (Denmark, Norway, and Italy). *Nordic Journal of Psychiatry, 70(5), 374–379.*

Chad-Friedman, E., Coleman, S., Traeger, L. N., Pirl, W. F., Goldman, R., Atlas, S. J., & Park, E. R. (2017). Psychological distress associated with cancer screening: a systematic review. *Cancer*, *123*(20), 3882-3894.

Chan-Olmsted, S., Chen, H., & Kim, H. J. (2024). In smartness we trust: consumer experience, smart device personalization and privacy balance. Journal of Consumer Marketing.

Chhetri, C., & Motti, V. (2022). “I mute my echo when I talk politics”: Connecting Smart Home Device Users’ Concerns to Privacy Harms Taxonomy. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 66, No. 1, pp. 2083-2087). Sage CA: Los Angeles, CA: SAGE Publications.

Choi, Y. K., Thompson, H. J., & Demiris, G. (2021). Internet-of-things smart home technology to support aging-in-place: older adults' perceptions and attitudes. *Journal of Gerontological Nursing*, *47*(4), 15-21.

Cobb, C., Bhagavatula, S., Garrett, K. A., Hoffman, A., Rao, V., & Bauer, L. (2021). “I would have to evaluate their objections”: Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*.

Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet of Things Journal*, *7*(10), 10102-10110.

DeFrank, J. T., Barclay, C., Sheridan, S., Brewer, N. T., Gilliam, M., Moon, A. M., ... & Harris, R. (2015). The psychological harms of screening: the evidence we have versus the evidence we need. *Journal of general internal medicine*, *30*, 242-248.

Dermody, G., Fritz, R., Glass, C., Dunham, M., & Whitehead, L. (2024). Family caregiver readiness to adopt smart home technology to monitor care—Dependent older adults: A qualitative exploratory study. *Journal of Advanced Nursing*, *80*(2), 628-643.

Despres, T., Constantino, M. A., Lizola, N. Z., Romero, G. S., He, S., Zhan, X., ... & Bernd, J. (2024). " My Best Friend's Husband Sees and Knows Everything": A Cross-Contextual and Cross-Country Approach to Understanding Smart Home Privacy. *Proceedings on Privacy Enhancing Technologies*.

Dillard, J. (2008). A slaughterhouse nightmare: Psychological harm suffered by slaughterhouse employees and the possibility of redress through legal reform. Georgetown Journal on Poverty Law & Policy, 15(2), 398.

Evangelakos, E. A., Kandris, D., Rountos, D., Tselikis, G., & Anastasiadis, E. (2022). Energy sustainability in wireless sensor networks: an analytical survey. *Journal of Low Power Electronics and Applications*, *12*(4), 65.

Farhadloo, M., Asvadi, S., & Khorasani, K. (2024). Potential vulnerabilities associated with emerging technologies: insights from a systematic literature review. *Management Review Quarterly*, 1-44.

Farsi, M., Elhosseini, M.A., Badawy, M., Arafat Ali, H., & Eldin, Z. H. (2019). Deployment Techniques in Wireless Sensor Networks, Coverage and Connectivity: A Survey. IEEE Access, 7, 28940–28954

Fokas, K. F., & Brovko, J. M. (2020). Assessing symptom validity in psychological injury evaluations using the MMPI-2-RF and the PAI: An updated review. *Psychological Injury and Law*, *13*(4), 370-382.

Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., ... & Zorn, B. (2020). Safety, security, and privacy threats posed by accelerating trends in the internet of things. *arXiv preprint arXiv:2008.00017*.

Gai, A., Azam, S., Shanmugam, B., Jonkman, M., & De Boer, F. (2018). Categorisation of security threats for smart home appliances. In *2018 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-5). IEEE.

Gale, A. (2019). Ethical issues in psychological research. In *Companion Encyclopedia of Psychology* (pp. 1156-1176). Routledge.

Ghorayeb, A., Comber, R., & Gooberman-Hill, R. (2021). Older adults' perspectives of smart home technology: Are we developing the technology that older people want?. *International journal of human-computer studies*, *147*, 102571.

Goldenson, J., & Josefowitz, N. (2021). Remote forensic psychological assessment in civil cases: considerations for experts assessing harms from early life abuse. *Psychological injury and law*, *14*(2), 89-103.

Gøthesen, S., Haddara, M., & Kumar, K. N. (2023). Empowering homes with intelligence: An investigation of smart home technology adoption and usage. *Internet of Things*, *24*, 100944.

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. *Energies*, *15*(19), 6984.

Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L., & Kantzavelou, I. (2020). Smart homes: security challenges and privacy concerns. *arXiv preprint arXiv:2010.15394*.

Haney, J. M., & Furman, S. M. (2023). User perceptions and experiences with smart home updates. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 2867-2884). IEEE.

Hannan Bin Azhar, M. A., Smith, D., & Cain, A. (2023). Spying on Kids' Smart Devices: Beware of Security Vulnerabilities!. In *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022* (pp. 123-140). Cham: Springer International Publishing.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398-428.

Helwig, C. C., Hildebrandt, C., & Turiel, E. (1995). Children's judgments about psychological harm in social context. *Child development*, *66*(6), 1680-1693.

Helwig, C. C., Zelazo, P. D., & Wilson, M. (2001). Children's judgments of psychological harm in normal and noncanonical situations. *Child development*, *72*(1), 66-81.

Hickey, B. A., Chalmers, T., Newton, P., Lin, C. T., Sibbritt, D., McLachlan, C. S., ... & Lal, S. (2021). Smart devices and wearable technologies to detect and monitor mental health conditions and stress: A systematic review. *Sensors*, *21*(10), 3461.

Humber, N., Emsley, R., Pratt, D., & Tarrier, N. (2013). Anger as a predictor of psychological distress and self-harm ideation in inmates: A structured self-assessment diary study. *Psychiatry research*, *210*(1), 166-173.

Huang, C. (2010). Internet use and psychological well-being: A meta-analysis. *Cyberpsychology, behavior, and social networking*, *13*(3), 241-249.

Islam, M. I., Yunus, F. M., Kabir, E., & Khanam, R. (2022). Evaluating risk and protective factors for suicidality and self-harm in Australian adolescents with traditional bullying and cyberbullying victimizations. *American journal of health promotion*, *36*(1), 73-83.

Iten, R., Wagner, J., & Zeier Röschmann, A. (2021). On the identification, evaluation and treatment of risks in smart homes: a systematic literature review. *Risks*, *9*(6), 113.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719-733.

Jaspers, E. D., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255-265.

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., ... & Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. *Journal of medical internet research*, *20*(4), e9044.

Johnson, W. B., Johnson, S. J., Sullivan, G. R., Bongar, B., Miller, L., & Sammons, M. T. (2011). Psychology in extremis: Preventing problems of professional competence in dangerous practice settings. *Professional Psychology: Research and Practice*, *42*(1), 94-104.

Jonsson, U., Alaie, I., Parling, T., & Arnberg, F. K. (2014). Reporting of harms in randomized controlled trials of psychological interventions for mental and behavioral disorders: a review of current practice. *Contemporary clinical trials*, *38*(1), 1-8.

Kandris, D., Tselikis, G., Anastasiadis, E., Panaousis, E., & Dagiuklas, T. (2017). COALA: a protocol for the avoidance and alleviation of congestion in wireless sensor networks. *Sensors*, *17*(11), 2502.

Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. *Global Transitions Proceedings*, *2*(2), 362-367.

Kessler, R. C., Andrews, G., Colpe, L. J., Hiripi, E., Mroczek, D. K., Normand, S. L., ... & Zaslavsky, A. M. (2002). Short screening scales to monitor population prevalences and trends in non-specific psychological distress. *Psychological medicine*, *32*(6), 959-976.

Kennedy, M. R., Huxtable, R., Birchley, G., Ives, J., & Craddock, I. (2021). "A Question of Trust" and "a Leap of Faith"—Study Participants' Perspectives on Consent, Privacy, and Trust in Smart Home Research: Qualitative Study. *JMIR mHealth and uHealth*, *9*(11), e25227.

Kirkøen, B., Berstad, P., Botteri, E., Åvitsland, T. L., Ossum, A. M., De Lange, T., ... & Bernklev, T. (2016). Do no harm: no psychological harm from colorectal cancer screening. *British journal of cancer*, *114*(5), 497-504.

Koch, W. J., Douglas, K. S., Nicholls, T. L., & O'Neill, M. L. (2005). *Psychological injuries: Forensic assessment, treatment, and law*. Oxford University Press.

Korneeva, E., Olinder, N., & Strielkowski, W. (2021). Consumer attitudes to the smart home technologies and the internet of things (IOT). *Energies*, *14*(23), 7913.

Kuaban, G. S., Gelenbe, E., Czachórski, T., Czekalski, P., & Tangka, J. K. (2023). Modelling of the energy depletion process and battery depletion attacks for battery-powered internet of things (iot) devices. *Sensors*, *23*(13), 6183.

Lee, C., Zappaterra, L., Choi, K., & Choi, H. A. (2014). Securing smart home: Technologies, security challenges, and security requirements. In *2014 IEEE Conference on Communications and Network Security* (pp. 67-72). IEEE.

Lee, Y., & Lim, Y. K. (2024). How We Use Together: Coordinating Individual Preferences for Using Shared Devices at Home. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (pp. 3407-3418).

Lilienfeld, S. O. (2007). Psychological treatments that cause harm. *Perspectives on psychological science*, *2*(1), 53-70.

Li, W., Logenthiran, T., Phan, V. T., & Woo, W. L. (2019). A novel smart energy theft system (SETS) for IoT-based smart home. *IEEE Internet of Things Journal*, *6*(3), 5531-5539.

Lim, H., & Lee, H. (2021). Cyberbullying: Its social and psychological harms among schoolers. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(1), 25-45.

Lim, H., & Lee, H. (2022). Its Social and Psychological Harms among Schoolers1. *Interpersonal Violence Against Children and Youth*, 109.

Linebarger, P. M. A. (1946). *A Syllabus of Psychological Warfare*. Intelligence Division, Propaganda Branch, WDGS.

Lippke, S., Dahmen, A., Gao, L., Guza, E., & Nigg, C. R. (2021). To what extent is internet activity predictive of psychological well-being?. *Psychology research and behavior management*, 207-219.

Litwiller, B. J., & Brausch, A. M. (2013). Cyber bullying and physical bullying in adolescent suicide: the role of violent behavior and substance use. *Journal of youth and adolescence*, *42*, 675-684.

Lupton, D. (2020). The internet of things: social dimensions. *Sociology Compass*, *14*(4), e12770.

Lutolf, R. (1992). Smart Home concept and the integration of energy meters into a home based system. In *Seventh international conference on metering apparatus and tariffs for electricity supply* (pp. 277–278). IEEE.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(5), 164-173.

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, *138*, 139-154.

Marshall, K. G. (1996). Prevention. How much harm? How much benefit? 3. Physical, psychological and social harm. *CMAJ: Canadian Medical Association Journal*, *155*(2), 169.

Massé, R. (2000). Qualitative and quantitative analyses of psychological distress: Methodological complementarity and ontological incommensurability. Qualitative Health Research, 10(3), 411–423.

McGorrery, P. G. (2020). *Causing Psychological Harm: A Criminal Offence?* (Doctoral dissertation, Deakin University).

Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y., & Shabtai, A. (2020). A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Computers & Security*, *97*, 101968.

Mihalopoulos, C., Magnus, A., Lal, A., Dell, L., Forbes, D., & Phelps, A. (2015). Is implementation of the 2013 Australian treatment guidelines for posttraumatic stress disorder cost-effective compared to current practice? A cost-utility analysis using QALYs and DALYs. *Australian & New Zealand Journal of Psychiatry*, *49*(4), 360-376.

Moh, P., Datta, P., Warford, N., Bates, A., Malkin, N., & Mazurek, M. L. (2023). Characterizing everyday misuse of smart home devices. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 2835-2849). IEEE.

Montes, Á., Sanmarco, J., Novo, M., Cea, B., & Arce, R. (2022). Estimating the psychological harm consequence of bullying victimization: a meta-analytic review for forensic evaluation. *International journal of environmental research and public health*, *19*(21), 13852.

Nakas, C., Kandris, D., & Visvardis, G. (2020). Energy efficient routing in wireless sensor networks: A comprehensive survey. *Algorithms*, *13*(3), 72.

National Health and Medical Research Council, Australian Research Council and Universities Australia (2023). National Statement on Ethical Conduct in Human Research. Canberra: National Health and Medical Research Council.

Oates, J., Carpenter, D., Fisher, M., Goodson, S., Hannah, B., Kwiatowski, R., Prutton, K., Reeves, D., & Wainwright, T. (2021). BPS code of human research ethics. British Psychological Society. https://www.bps.org.uk/guideline/bps-code-human-research-ethics

Olabode, S., Owens, R., Zhang, V. N., Copilah-Ali, J., Kolomeets, M., Wu, H., ... & Chambers, D. (2023). Complex online harms and the smart home: A scoping review. *Future Generation Computer Systems*.

Olson, R. E. (2023). Emotions in human research ethics guidelines: Beyond risk, harm and pathology. *Qualitative Research*, *23*(3), 526-544.

Orfanos, V. A., Kaminaris, S. D., Papageorgas, P., Piromalis, D., & Kandris, D. (2023). A comprehensive review of IoT networking technologies for smart home automation applications. *Journal of Sensor and Actuator Networks*, *12*(2), 30.

Packard, V. O. (1957). *The hidden persuaders*. Daviv McKay. New York. US.

Pal, D., Zhang, X., & Siyal, S. (2021). Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technology in Society*, *66*, 101683.

Panwar, N., Sharma, S., Mehrotra, S., Krzywiecki, Ł., & Venkatasubramanian, N. (2019). Smart home survey on security and privacy. *arXiv preprint arXiv:1904.05476*.

Paupini, C., Van der Zeeuw, A., & Teigen, H. F. (2022). Trust in the institution and privacy management of Internet of Things devices. A comparative case study of Dutch and Norwegian households. *Technology in Society*, *70*, 102026.

Peters, H. J., Schwenk, H. N., Ahlstrom, Z. R., & McIalwain, L. N. (2017). Microaggressions: The experience of individuals with mental illness. *Counselling Psychology Quarterly*, *30*(1), 86-112.

Phillips, M. R. (2009). Is distress a symptom of mental disorders, a marker of impairment, both or neither? *World Psychiatry*, *8*(2), 91-92.

Raff, S., Rose, S., & Huynh, T. (2024). Perceived creepiness in response to smart home assistants: A multi-method study. *International Journal of Information Management*, *74*, 102720.

Ridner, S. H. (2004). Psychological distress: concept analysis. *Journal of advanced nursing*, *45*(5), 536-545.

Rutledge, R. L., Massey, A. K., & Antón, A. I. (2016). Privacy impacts of IoT devices: A SmartTV case study. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)* (pp. 261-270). IEEE.

Sáncheza, G., Ampudiab, A., Jiméneza, F., & Amado, B. (2017). Contrasting the efficacy of the MMPI-2-RF overreporting scales in the detection of malingering. *The European Journal of Psychology Applied to Legal Context, 9*, 51–56.

Saxena, U., Sodhi, J. S., & Singh, Y. (2020). An analysis of DDoS attacks in a smart home networks. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 272-276). IEEE.

Schein, E. H., & Bennis, W. (1965). Personal and organizational change through group methods. New York: Wiley.

Schlenker, B. R., & Forsyth, D. R. (1977). On the ethics of psychological research. *Journal of Experimental Social Psychology*, *13*(4), 369-396.

Schneider, S. K., O'donnell, L., Stueve, A., & Coulter, R. W. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *American journal of public health*, *102*(1), 171-177.

Schultz, D. P. (1969). The human subject in psychological research. *Psychological Bulletin, 72*(3), 214–228.

Schomakers, E. M., Biermann, H., & Ziefle, M. (2021). Users' preferences for smart home automation–investigating aspects of privacy and trust. *Telematics and Informatics*, *64*, 101689.

Serrenho, T., & Bertoldi, P. (2019). Smart home and appliances: State of the art. *Energy, communications, protocols, standards. Brussels: JRC technical reports*, 2-36.

Shalawadi, S. B., Echtler, F., & Raptis, D. (2024). Dr. Convenience Love or: How I Learned to Stop Worrying and Love my Voice Assistant. In *Nordic Human-Computer Interaction Conference (NordiCHI'24), Uppsala, Sweden.*

Shandler, R., Gross, M. L., & Canetti, D. (2023). Cyberattacks, psychological distress, and military escalation: An internal meta-analysis. *Journal of Global Security Studies*, *8*(1), ogac042.

Sharma, N., Singh, B. M., & Singh, K. (2021). QoS-based energy-efficient protocols for wireless sensor network. *Sustainable Computing: Informatics and Systems*, *30*, 100425.

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device?-a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, *6*(1), 1-10.

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials*, *23*(2), 1125-1159.

Slade, J., & Alleyne, E. (2023). The psychological impact of slaughterhouse employment: A systematic literature review. *Trauma, Violence, & Abuse*, *24*(2), 429-440.

Slupska, J., & Tanczer, L. M. (2021). Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things. In *The Emerald international handbook of technology-facilitated violence and abuse* (pp. 663-688). Emerald Publishing Limited.

Smith, R., Palin, D., Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2020). Battery draining attacks against edge computing nodes in IoT networks. *Cyber-Physical Systems*, *6*(2), 96-116.

Smythe, H. H., & Seidman, M. (1957). Name calling: A significant factor in human relations. *Journal of Human Relations, 6, 71–77.*

Solaimani, S., Keijzer-Broers, W., & Bouwman, H. (2015). What we do–and don't–know about the Smart Home: an analysis of the Smart Home literature. *Indoor and Built Environment*, *24*(3), 370-383.

Somasundaram, K., & Selvam, K. (2018). IOT–attacks and challenges. *Int. J. Eng. Tech. Res*, *8*(9), 9-12.

Spilsbury, B., Robertson, R., & Lett, M. H. (1936). A MEDICO-LEGAL INSTITUTE. *British Medical Journal, 229.*

Statista. (2024). Digital Markets: Smart Home – Worldwide. https://www.statista.com/outlook/dmo/smart-home/worldwide.

Sun, Y., & Li, S. (2021). A systematic review of the research framework and evolution of smart homes based on the internet of things. *Telecommunication Systems*, 77(3), 597-623.

Tabassum, M., Kosinski, T., & Lipford, H. R. (2019). " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 435-450).

Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-9). IET.

Taplin, R. (2020). *Cyber risk, intellectual property theft and cyberwarfare: Asia, Europe and the USA*. Routledge.

Task Force on Community Preventive Services. (2008). Recommendations to reduce psychological harm from traumatic events among children and adolescents. *American journal of preventive medicine*, *35*(3), 314-316.

Trimananda, R., Younis, A., Wang, B., Xu, B., Demsky, B., & Xu, G. (2018). Vigilia: Securing smart home edge computing. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 74-89). IEEE.

Turner, S., Pattnaik, N., Nurse, J. R., & Li, S. (2022). " You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1-34.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, *4*(1), 18.

Ukpana, I. (2024) Smart Home Statistics: Key Insights and Trends. https://www.greenmatch.co.uk/blog/smart-home-statistics

United Nations (2023). 'The regulatory compliance of products with embedded artificial intelligence or other digital technologies' working paper. https://unece.org/sites/default/files/2023-12/2023-9-Compliance-AI_Eng.pdf

United Kingdom Research and Innovation UKRI (2024). https://www.ukri.org/councils/esrc/guidance-for-applicants/research-ethics-guidance/risk-and-benefit/

Vilariño, M., Amado, B. G., Seijo, D., Selaya, A., & Arce, R. (2022). Consequences of child maltreatment victimisation in internalising and externalising mental health problems. *Legal and Criminological Psychology*, *27*(2), 182-193.

Vilariño, M., Arce, R., & Fariña, F. (2013). Forensic-clinical interview: Reliability and validity for the evaluation of psychological injury. *The European Journal of Psychology Applied to Legal Context*, *5*(1), 1-21.

Vuorre, M., & Przybylski, A. K. (2023, preprint). *A multiverse analysis of the associations between internet use and well-being*. PsyArXiv Preprints. https://doi.org/10.31234/osf.io/jp5nd

Wethington, H. R., Hahn, R. A., Fuqua-Whitley, D. S., Sipe, T. A., Crosby, A. E., Johnson, R. L., ... & Task Force on Community Preventive Services. (2008). The effectiveness of interventions to reduce psychological harm from traumatic events among children and adolescents: a systematic review. *American journal of preventive medicine*, *35*(3), 287-313.

Wissler, R. L., Hart, A. J., & Saks, M. J. (2017). Decision making about general damages: A comparison of jurors, judges, and lawyers. In *The Right to a Fair Trial* (pp. 355-430). Routledge.

Wygant, D. B., & Lareau, C. R. (2015). Civil and criminal forensic psychological assessment: Similarities and unique challenges. *Psychological injury and law*, *8*, 11-26.

Young, G., Foote, W. E., Kerig, P. K., Mailis, A., Brovko, J., Kohutis, E. A., ... & Goodman-Delahunty, J. (2020). Introducing psychological injury and law. *Psychological Injury and Law*, *13*, 452-463.

Zimmermann, V., Gerber, P., Marky, K., Böck, L., & Kirchbuchner, F. (2019). Assessing users' privacy and security concerns of smart home technologies. *i-com*, *18*(3), 197-216.

Table 1. Definitions of Psychological harm as it presents in a variety of domains

Context	Definition	Source
Cyber attacks	Psychological harm/Extreme psychological distress "visceral anxiety, enduring anger, and heightened threat perception… cyberattacks cause equally high levels of psychological distress as conventional terrorism and political violence ."	Shandler et al (2023) Page 3
Cyber bullying	"Traumatic exposures may also result in psychological harm such as anxiety disorders and symptoms, including posttraumatic stress disorder (PTSD) and PTSD symptoms; depressive disorders and symptoms; externalizing disorders and symptoms (e.g., acting out, aggressive and impulsive behavior); internalizing disorders and symptoms (e.g., withdrawn, depressed, or fearful behavior); suicidal ideation or behavior; substance abuse; and childhood traumatic grief or complicated grief."	Wethington et al (2008) page 287
Substance abuse	"Posttraumatic stress disorder (PTSD) is the forensic psychological evidence of psychological Harm"	Montes et al (2022) Page 2.
Clinical, Medical interventions	"Anxiety over anticipated adverse effects of procedures and over test results/Excessive awareness of health; Anxiety induced over positive results/false assurances over negative results; Distress resulting from actual or anticipated physical harm"	Marshall (1996) Page 170.
Children Bullying	"In the case of psychological harm, the victim must first interpret the action in order to experience the consequence (as, e.g., a verbal insult)…an act of psychological harm may be trans- formed into a nonharmful act, and vice- versa, through changes in the recipient's interpretation….judgments about psychological harm may interact with judgments about social contexts in complex ways, posing special problems for the development of these concepts"	*Helwig et al (1995). Page 1681
Children Bullying	"…psychological harm is more conspicuously mediated by a person's interpretation… to experience psychological harm, a person must interpret an act as harmful or negatively intended. To the extent that individuals' interpretations of acts vary, the relation between acts and their consequences is less predictable. In psychological harm, the harm that occurs is a direct function of the interpretation placed upon the act by the recipient (e.g., as in interpreting an utterance as an insult), and any act of psychological harm may be wholly transformed into a nonharmful event by changes in the recipient's interpretation (e.g., by reinterpreting an act as a compliment rather than an insult)."	Helwig et al (2001). Page 66-67
Clinical, Medical Treatment	"Psychological harms may be important either by carrying a high burden or by occurring very frequently (or both). Some psychological harms may not be severe enough to classify as pathology, but the distress may affect large numbers of people and thus should not be routinely dismissed as small. Other harms may lead to severe psychological problems for a small number of predisposed people. In neither case should clinicians draw the conclusion that harms are trivial and can be discounted"	DeFrank et al (2015). Page 247
Employees working in adverse conditions	"psychological harm such as depression may be compensated only if there is "a finding either that claimant's work performance (as distinguished from the mere job description) was unusually stressful for that kind of a job or a finding that an unusual event occurred making the job more stressful than it had been"	Dillard (2008). Page 405-406
Micro-aggressions	"Understanding microaggressions is important because they can result in emotional and psychological harm. Some examples of harm include increased feelings of frustration, anger, anxiety, depression [..], low self-esteem, self-doubt, isolation […], feeling alienated, invisible, and as if one's cultural values are constantly invalidated […]. Further, microaggressions lead to perceptions of hostility in school environments […] and poor work relationships […]".	Peters et al., (2017). Page 88.
Traumatic events	"The psychological harms that may result from exposure to such traumatic events include post-traumatic stress disorder (PTSD) and PTSD symptoms, depressive disorders and symptoms, externalizing behaviors, internalizing behaviors, suicidal ideation, and complicated grief. Traumatic exposures may lead to other health consequences as well, including risk-taking behavior and chronic physical disorders	Task Force on Community Preventive Services. (2008) Page 314

Table 2. Assessment tool for measuring psychological distress when experiencing cyberbullying

Kessler et al (2002)	Lim & Lee (2022)
1. Did you feel tired out for no good reason. 2. Did you feel nervous. 3. Did you feel so nervous that nothing could calm you down. 4. Did you feel hopeless. 5. Did you feel restless or fidgety. 6. Did you feel so restless that you could not sit still. 7. Did you feel depressed. 8. Did you feel that everything was an effort. 9. Did you feel so sad that nothing could cheer you up. 10. Did you feel worthless	1. Did you avoid any activities at school because you thought someone might attack or harm you? 2. Did you avoid any class at school because you thought someone might attack or harm you? 3. Did you stay home from school because you thought someone might attach or harm you? 4. During the last four weeks, did you skip any classes? 5. How often are you afraid that someone will attack or harm you on a school building/property? 6. How often are you afraid that someone will attack or harm you on a school bus or on the way to and from school? 7. Besides the times you are on school property or going to school, how often are you afraid that someone will harm you?

Table 3. Properties of psychological distress used in assessments

Ridner's (2004) Nursing assessment of psychological distress		Massé (2000) specifies six types of characteristics that can identify psychological distress	
Defining attribute	Signs	Defining attribute	Signs
Perceived inability to cope	Failure to verbalize ways to address problem, dependence on others to make decisions, hopelessness, avoidance of issue	Negative perceptions of the future	demoralization and pessimism toward the future consisting in a deep conviction that, in the future, things can only get worse
Change in emotional status	Anxiety, irritableness, depression, withdrawal from others, hyperactivity, tearfulness, inappropriate laughter	Emotional state of Helplessness	anguish and stress conceived as an internal suffering entailing preoccupations, nervous tension, and feelings of powerlessness
Discomfort	Sadness, aches, pain, anger, hostility	Negative perceptions of self	self-depreciation consisting in the tendency of some people to be very self-critical and to put the blame on themselves
Communication of discomfort	Verbal = expressing lack of hope for future, fearful, complaining of pain, insomnia, silence; Physical = scowling, frowning, restless, neglectful of appearance, avoiding eye contact	Social withdrawal	social withdrawal and social isolation when people do not want to socialize with others, preferring to escape from social life
Harm	Pain, change in vital signs, suicide gesture, desire to leave against medical advice	Negative Physical states	somatization characterized by common signs such as physical exhaustion, loss of energy, and fatigue
		withdrawal into oneself	individual's perceived incapacity to control his or her life and to adjust to his or her social environment

Figure 1. Aldahmani et al., 2023 representation of CPIC grouped into different functionalities within a home.